611-TD-567-001

EOSDIS Core System Project

M&O Procedures: Section 3—System Administration

Interim Update

April 2000

Raytheon Systems Company
Upper Marlboro, Maryland

Preface

This document is an interim update to the Mission Operations Procedures Manual for the ECS Project, document number 611-CD-500-001. This document has not been submitted to NASA for approval, and should be considered unofficial.

The document has been updated to include information relevant to ECS Release 5B.

Any questions should be addressed to:

Data Management Office
The ECS Project Office
Raytheon Systems Company
1616 McCormick Drive
Upper Marlboro, Maryland 20774-5301

This page intentionally left blank.

3. System Administration

This section covers the procedures necessary for the System Administrator (SA) and/or Operator (OPR) to manage and operate the system.

Detailed procedures for tasks performed by the System Administrator and/or Operator are provided in the sections that follow. The procedures assume that the administrator and/or operator is authorized and has proper access privileges to perform the tasks (i.e., root) and that the SA and/or OPR has been properly trained in all aspects of the system.

Each procedure outlined will have an **Activity Checklist** table that will provide an overview of the task to be completed. The outline of the **Activity Checklist** is as follows:

Column one - ***Order*** shows the order in which tasks should be accomplished.

Column two - ***Role*** lists the Role/Manager/Operator responsible for performing the task.

Column three - ***Task*** provides a brief explanation of the task.

Column four - ***Section*** provides the Procedure (P) section number or Instruction (I) section number where details for performing the task can be found.

Column five - ***Complete?*** is used as a checklist to keep track of which task steps have been completed.

The following is the **Activity Checklist** table that provides an overview of the overall system administration processes and who performs them

Table 3.1. System Administration - Activity Checklist

Order	Role	Task	Section	Complete?
1	OPR	Secure Shell	(I) 3.1	
2	OPR	Starup/Shutdown	(I) 3.2	
3	OPR	System Backup and Restore	(I) 3.3	
4	SA	User Administration	(I) 3.4	
5	SA	Installing a New Workstation	(I) 3.5	
6	SA	DCE Configuration	(I) 3.6	
7	SA/ OPR	Installing CUSTOM Software/System Monitoring	(I) 3.7	

For procedures outlined in this section, there are corresponding **QUICK STEP** procedures immediately following in this chapter. The **QUICK STEP** procedures are designed for persons who have ***prior training or are experienced system administrators with prior system administration experience.*** The ***QUICK STEP*** procedures should be used by ***experienced persons ONLY***.

3.1 Secure Shell

Secure Shell (ssh) is a set of programs that greatly improve network security. The primary need for it on ECS is to allow secure, interactive access to ECS DAACs without needing burdensome procedures and mechanisms and additional hardware.

Secure in this context means not sending passwords "in the clear" so that hackers may intercept them and also provides encryption of the entire session.

Secure Shell is to be used for any inter-access among system platforms and between DAACs

Table 3.1-1. Secure Shell - Activity Checklist

Order	Role	Task	Section	Complete?
1	OPS	Initiating sshsetup	(I) 3.1.1	
2	OPR	Setting up remote access ssh	(I) 3.1.2	
3	OPR	Changing Your Passphrase	(I) 3.1.3	

3.1.1 Setting Up ssh

Most users will start from the same host whether from an X terminal, a UNIX workstation or a PC. Prior to executing ssh commands, use **setenv DISPLAY <IP address>:0.0** at your local host. To ensure system security, do not use the **setenv DISPLAY** command on subsequent hosts accessed via ssh. The process is started by running the sshsetup script which will enable ssh to other hosts from which one may use the same home directory. The only thing you need to do before executing the script is to pick a good passphrase of at least 10 characters. You can, and should, use spaces and multiple words with numbers and misspellings and special characters. Note that passwords are NOT echoed back to the screen.

To initialize Secure Shell Access (ssh), execute the procedure steps that follow:

1 Login to your normal Unix workstation where your home directory resides.

2 Initiate Secure Shell setup by typing **/tools/bin/sshsetup**, then press Return/Enter.

- You will see an information statement:

Use a passphrase of at least 10 characters which should include numbers or special characters and MAY include spaces

3 At the prompt "New passphrase:" **enter your passphrase <enter>**.

4 At the prompt "Retype new passphrase:" **re-enter your passphrase <enter>**.

- You will then see:

```
Initializing random number generator...

Generating p:  Please wait while the program completes ...

%
```

- This establishes the .ssh sub-directory in your <username>/home directory, creates the local ssh key, and creates the necessary files.

3.1.2 Remote ssh Access

If you need to access a host with a different home directory, you will need to run the sshremote script. This script sets up the destination host with the new set of keys and transfers the source (local) key to the destination and the destination key to the source. You must have an existing account on the remote host.

To set up remote access shell (ssh), execute the procedure steps that follow:

1 Login into your normal Unix workstation where your home directory resides.

2 Initiate Secure Shell remote setup by typing **/tools/bin/sshremote**, then press Return/Enter.

- You will see the following prompt:

```
You have a local passphrase. Do you want to setup for:

1   VATC

2   EDF

3   MiniDAAC

4   GSFC DAAC

5   GSFC M and O

6   EDC DAAC

7   EDC M and O

8   LaRC DAAC

9   LaRC M and O

10  NSIDC DAAC
```

```
11  NSIDC M and O

12  Exit from script

Select:
```

3 At the "Select" prompt, type in the corresponding number to the desired host, then press Return/Enter.

- You will receive a prompt similar to the following for the VATC:

```
Working...
```

4 At the prompt "Enter passphrase for RSA key '<username>@<hostname>': Type in your **passphrase** and then press Return/Enter.

- A prompt similar to the following will be displayed:

```
Last login: Thu Jul  9 10:41:13 1998 from echuser.east.hit

        No mail.

Sun Microsystems Inc.   SunOS 5.5.1     Generic May 1996

t1code1{username}1:
```

5 At the prompt "Press <ctrl>a to run sshsetup and exit <enter> to logoff t1code1u", type **<ctrl>-a** to initiate the sshsetup script on the remote host

- You will see an information statement:

```
Use a passphrase of at least 10 characters which should include numbers

or special characters and MAY include spaces
```

6 At the prompt "New passphrase:" **enter your passphrase <enter>**.

7 At the prompt "Retype new passphrase:" **re-enter your passphrase <enter>**.

- You will then see:

```
Initializing random number generator...

Generating p:  Please wait while the program completes ...

%
```

8 At the "t1code1" prompt type **exit**, the press Return/Enter.

- The following information will be displayed:

```
Updating locally...

Updating t1code1u.ecs.nasa.gov

 %
```

- This establishes the ssh key at the remote host and exchanges key information with your local host.

Note: The ssh keys at remote sites can be different from the local host ssh key.

3.1.3 Changing Your Passphrase

Another script has been developed to change your passphrase on the local host and then transfer the key to the other environments. The ssh keys for remote hosts will have to be changed separately. Use the following procedure to change your passphrase:

To change your Secure Shell Passphrase, execute the procedure steps that follow:

1 Login to your normal Unix workstation where your home directory resides.

- Initiate passphrase change by typing **/tools/bin/sshchpass**, then press Return/Enter.
- You will see an information statement:

```
Use a passphrase of at least 10 characters which should include numbers

or special characters and MAY include spaces
```

2 At the prompt "Old passphrase:" **enter your old passphrase <enter>**

3 At the prompt "New passphrase:" **enter your passphrase <enter>**.

4 At the prompt "Retype new passphrase:" **re-enter your passphrase <enter>**.

- You will then see an information prompt similar to the following:

```
ssh-keygen will now be executed. Please wait for the prompt to Return!

/home/bpeters/.ssh/authorized_keys permissions have already been set.


%
```

3.2 System Startup and Shutdown

The Startup and Shutdown processes begin when it has been determined by the DAAC Operations Supervisor or his designee that it is necessary to stop or start the system. The least impacting method is determined and users are appropriately notified.

When determining the least impacting way to perform the startup or shutdown, the OPR, along with the Operations Supervisor takes into consideration whether only specific server software packages would need to be started/stopped or an entire system startup/shutdown is required.

Once these steps have been taken, the shutdown or startup is performed.

The **Activity Checklist** table that follows provides an overview of the startup and shutdown processes.

Table 3.2-1. Startup/Shutdown - Activity Checklist

Order	Role	Task	Section	Complete?
1	OPS Sup	Determine that Startup/Shutdown is necessary.	(I) 3.2	
2	OPR	Determine the Least Impacting Way to Perform the Startup/Shutdown.	(I) 3.2	
3	OPR	Notify Those Effected by the Startup/Shutdown.	(I) 3.2	
4	OPR	Perform the Startup/Shutdown	(P) 3.2	

3.2.1 Startup

Startup means that power to the system is restored and the system is being taken to a fully useable and operational state.

3.2.1.1 Cold - By Subsystem

A cold startup means that power to the system has been previously powered off and the system(s) is being restarted from this cold state. The System Startup process begins after a previously completed shutdown, either scheduled or emergency. The System Startup is done in sequential order by subsystem. This startup sequence is predetermined by the SA.

This procedure assumes that the OPR has been properly trained to startup all aspects of the system and that the system is currently powered off (due to a normal or emergency shutdown).

The procedure assumes that the Startup has been scheduled well in advance, all planning involved has been concluded well in advance and all other Distributed Active Archive Centers (DAACs) have been notified of the system returning to an on-line state.

This section explains how to perform a cold system startup by subsystem. The sequence of the execution of the steps below are VERY IMPORTANT. To begin a cold system startup, execute the procedure steps that follow:

1 The **sequence** of booting the machines is **IMPORTANT**:

- ***Remember to power on peripherals before powering on each CPU***
- ***Monitor each system Boot Up activity on that system's monitor***
- *****The DNS and NIS servers must be booted FIRST***
- ***Once each system has booted without error, proceed to the next machine***
- Boot the machines per Table 3.2-2

2 Continue booting the remaining machines

Table 3.2-2 presents the cold system startup machine boot sequence, however, the machine names are to be added once identified at each DAAC, per their specific baseline by the SA.

Table 3.2-2. Cold System Startup - Machine Boot Sequence

Step	What to Enter or Select	Action to Take (Server)	Machine Name
1	(No entry)	NIS Master	**x0css02**
2	(No entry)	DCE Servers	**x0css02**
3	(No entry)	DNS Master	**x0css02**
4	(No entry)	Clearcase Server(s)	**x0mss0x**
	(No entry)	Interface Server(s)	**x0ins0x**
5	(No entry)	MSS: *Tivoli Server,* *HP Openview Server*	**x0mshxx**
6	(No entry)	DSS	**x0acs0x**
7	(No entry)	Ingest	**x0icg0x**
8	(No entry)	PDPS	**x0pls0x**
9	(No entry)	Others	

3.2.1.2 Warm - By Subsystem Startup

A warm startup means the system has been previously powered on, but the system(s) is not fully operational, either the system has had some service performed (i.e. single user mode) or is being rebooted to correct some minor malfunction. The System Startup is done in sequential order by subsystem. This startup sequence is predetermined by the software dependencies.

The order of the re-boot is contingent on software dependencies per site.

If the NIS/DCE servers service has been interrupted, the users will automatically be transferred to a backup server. Once the faulty server(s) has been repaired, re-establish connection with the primary NIS/DCE server by rebooting the Backup Server; the users would then be transferred back to the primary NIS/DCE server.

Table 3.2-3 presents the **QUICK STEP** procedure required to perform a warm system startup.

Table 3.2-3. Warm System Startup - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	determine software dependencies
2	(No entry)	reboot independent server(s)
3	(No entry)	reboot dependent server(s)

Note - in addition to warm system startup/reboot sequences, ECS servers which use the Sybase SQL server may need to be bounced whenever the SQL server is bounced. At present, this is certainly the case for all STMGT servers. That is, if the Sybase SQL server is stopped and restarted for any reason, all STMGT servers need to be stopped and restarted, once the Sybase SQL server has come back on-line.

3.2.1.3 Additional tasking - Updating leapsec.dat and utcpole.dat files

In addition to starting system servers there are essential tasks that System Administrators must perform on a regular basis.

In order to ensure proper operation of Program Generated Executives (PGEs), two files must be updated weekly with data transferred from the U.S. Naval Observatory. These files are ${PGSHOME}/database/common/TD/leapsec.dat and ${PGSHOME}/database/common/CSC/utcpole.dat. The update of these files is accomplished by executing leapsec_update.sh and utcpole_update.sh in the /tools/admin/exec directory with root privileges. It has not been determined yet if these tasks will be accomplished manually or via cron job scripting .

3.2.2 Shutdown

Shutdown means that the system is being removed from a fully useable and operational state and possibly, power to the system will be terminated. The types of shutdown would vary depending upon circumstances (i.e. shutdown to single user mode; shutdown to power off; etc.)

3.2.2.1 Normal - By Subsystem

The Normal System Shutdown process is performed at the discretion of the SA usually for a scheduled repair. The system shutdown is **normally performed in reverse order of the system startup.**

The procedures assume that the Shutdown has been scheduled well in advance, all planning involved has been concluded well in advance and the OPR/SA has been properly trained to shutdown all aspects of the system.

This section explains how to perform a normal system shutdown by subsystem**.**

3.2.2.1.1 Shutdown a Machine

The OPR must be logged in as root to perform a shutdown. To begin a normal system shutdown, execute the procedure steps that follow:

1 Login to the server as root.

2 Enter root password.

3 Type **wall** and press **Return**. Use **wall -a** on Sun machines to cross NFS mounts.

4 Type **This machine is being shutdown for *reason*. The anticipated length of down time is *xxx*. Please save your work and log off now. The machine will be coming down in *xxx* minutes. We are sorry for the inconvenience.** then press **Return.** Press **Control** and **D** keys **simultaneously**. Include your name and closest telephone number.

5 Wait at least five minutes.

6 Type **shutdown -g600 -i0 -y** UNIX prompt and press **Return**. (600 = Number of Seconds)

7 When the system is at the prompt it is safe to ***Power off*** all peripherals first, and then the CPU.

The servers should be shutdown in the reverse order of the startup:

1 Determine which machines are dependent on a server first:

- ***Once each system has stopped without error, power off peripherals***
- ***Proceed to the following machine***
- ***Follow steps 1-7 for Task: 3.2.2.1.1 Shutdown Machine*** *for* ***each*** *machine*

2 **Do NOT** turn power off on the **HP Systems**, instead bring them down to the halted mode, unless power is going to be lost for the entire facility.

3 The **NIS/DCE server** must be the **last system** to be shutdown.

Table 3.2-4 presents the **QUICK STEP** procedure required to perform a normal system shutdown.

Table 3.2-4. Normal System Shutdown - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	**determine subsystems and server dependencies**
2	(No entry)	**Login to the server as root**
3	**wall**	**Press Return**
4	**This machine is being shutdown for *reason*. The anticipated length of down time is *xxx*. Please save your work and log off now. The machine will be coming down in *xxx* minutes. We are sorry for the inconvenience.**	**Press Control and D keys simultaneously**

5	(No entry)	**Wait at least five minutes**
6	**shutdown -g600 -i0 -y** **- OR** **shutdown now -i0 -y**	**Press Return**
7	(No entry)	**Power off all peripherals and the CPU.**
8	(No entry)	**Repeat steps 2 through 7 above for all servers Table 3.2.2**

3.2.2.2 Emergency - By Subsystem

The Emergency System Shutdown process begins after it is determined that the system may fail during emergency situations (i.e., storms, power outages) by the System Administrator (SA). The Emergency System Shutdown is done in sequential order by subsystem. This shutdown sequence is predetermined by the SA.

The NIS/DCE servers must be the last system to shutdown.

Detailed procedures for tasks performed by the OPR/SA are provided in the sections that follow.

This section explains how to perform an emergency system shutdown by subsystem. The OPR must be logged in as root to perform a shutdown. To begin an emergency system shutdown, execute the procedure steps that follow:

1 Login to the server as root.

2 Enter root password.

3 Type **sync** at the UNIX prompt and hit **Return**.

Sync executes the sync system primitive. If the system is to be stopped, sync must be called to insure file system integrity. It will flush all previously unwritten system buffers out to disk, thus assuring that all file modifications up to that point will be saved.

4 Type **sync** again at the UNIX prompt and hit **Return**.

5 Type **halt** at the UNIX prompt and hit **Return**.

6 Once the halt has completed, turn the power switch on all the peripherals and the CPU off.

The servers should be shutdown in the following order:

1 Shutdown all client workstations.

2 ***Follow steps 1-7 for Task: 3.2.2.1.1 Shutdown Machine*** *for* ***<u>each</u>*** *machine*

3 Do **NOT** turn power off on the **HP Systems**, instead bring them down to the halted mode, unless power is going to be lost for the entire facility.

4 The **NIS/DCE servers** must be the **last systems** to shutdown.

In case of ***EXTREME emergency*** where time does not allow you to execute the above procedures, execute the following procedure steps for ***Sun machines ONLY.***

1 Login to the server as root.

2 Enter root password.

3 Hit the L1 or Stop key and the a key simultaneously.

4 Once returned to an **ok** or **>** prompt, turn the power switches on the CPU and all peripherals to off.

NOTE: The use of L1a does not ensure file system integrity. There is a very high risk of losing data when using this process.

Table 3.2-5 presents the **QUICK STEP** procedures required to perform a Emergency System Shutdown.

Table 3.2-5. Emergency System Shutdown - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	**determine subsystems and server dependencies**
2	(No entry)	**Login to server as root**
3	(No entry)	**Type sync at prompt and press enter**
4	(No entry)	**Type sync at prompt and press enter**
5	(No entry)	**Type halt at prompt and press enter**
6	(No entry)	**Turn power switches on CPU and all peripherals to off.**
7	(No entry)	**Repeat steps 2 through 5 above for all servers**

3.2.2.3 Server - By Server Software

The System Shutdown by Server Software process is performed by the OPR. The system shutdown is normally performed in reverse order of the system startup.

The procedures assume that the Shutdown has been scheduled well in advance, all planning involved has been concluded well in advance and the SA has been properly trained to shutdown all aspects of the system.

Table 3.2-6 presents the **QUICK STEP** procedure required to perform a normal system shutdown.

Table 3.2-6. Server System Shutdown - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	**determine software dependencies**
2	(No entry)	**shutdown dependent server(s)**

3	(No entry)	**shutdown independent server(s)**

3.3 System Backup and Restore

System Backup and Restore is the process of copying, either the entire or partial system, the information from the machine for safe keeping for a specific time period. Restore is the process of returning the data to the machine to allow operation to continue from a specific point in time. The OPR must be in the admin list to use Networker. This is not root privilege.

3.3.1 Incremental Backup

Non-scheduled incremental backups can be requested at any time by submitting a request for ***Incremental Backup*** to the **OPS supervisor**. The supervisor schedules the request with the OPR who performs the incremental backup. Afterwards, the OPR notifies the requester and supervisor that the incremental backup is complete.

The **Activity Checklist** table that follows provides an overview of the incremental backup processes.

Table 3.3-1. Incremental Backup - Activity Checklist

Order	Role	Task	Section	Complete ?
1	Requester	Submit Request for **Incremental** Backup to OPS Supervisor.	(I) 3.3.1	
2	OPS Super	Schedule Incremental Backup with OPR	(I) 3.3.1	
3	OPR	Perform Incremental Backup.	(P) 3.3.1	
4	OPR	Notify Requester and OPS Super when Incremental Backup is Complete.	(I) 3.3.1	

Detailed procedures for tasks performed by the OPR are provided in the sections that follow.

The procedures assume that the requester's request for an incremental backup has already been approved by DAAC Management. Incremental backups can be requested at any time by submitting a request for ***Full Backup*** to the **OPS supervisor**. In order to perform the procedure, the OPR must have obtained the following information from the requester:

a. **Name of machine to be backed up**

b. **Files/directories to be backed up (optional)**

To perform an incremental backup for the requester, execute the procedure steps that follow:

Note 1: If you run out of tapes at any time during this procedure, execute procedure 3.3.5.1 Labeling Tapes and then return to this procedure.

1 Log into the **machine to be backed up** by typing: **ssh *BackedUpSystemName***, then press **Return**.

2 At the Passphrase promt: enter ***YourPassphrase***, then press **Return**.

- Or press **Return** twice to get the Password prompt.

3 Enter ***YourPassword***, then press **Return.**

- Remember that ***YourPassword*** is case sensitive.
- You are authenticated as yourself and returned to the UNIX prompt.

4 Log in as root by typing: **su**, then press **Return**.

- A password prompt is displayed.

5 Enter the ***RootPassword***, then press **Return**.

- Remember that the ***RootPassword*** is case sensitive.
- You are authenticated as root and returned to the UNIX prompt.

6 Execute the NetWorker Administrative program by entering: **nwadmin &**, then press **Return**.

- A window opens for the NetWorker Administrative program.
- You are now able to perform an incremental backup.

7 Click Clients.

- Click Client Setup
- Click Host Being Backed Up
- Highlight the group to be Backed Up

8 Go to the **Customize** menu, select **Schedules**.

- The **Schedules** window opens.

9 Look at the button for today. If there is an **i** next to the date on this button, go to step 12.

- The **i** stands for incremental.
- The **f** stands for full.

Whichever is on the button for today is what kind of backup that will be done, unless it is overridden.

10 Click and hold the button for today, select **Overrides** from the resulting menu, select **Incremental** from the next resulting menu.

11 Click the **Apply** button.

12 Close the **Schedules** window by clicking in the upper left corner of the **Schedules** window and selecting **Close** from the resulting menu.

13 Click the **Group Control** button.

- The **Group Control** window opens.

14 Click the **Start** button.

- A **Notice** window opens.

15 Click the **OK** button.

- The **Notice** window closes.
- The regularly scheduled backup will still run (even though we are now doing a backup).

16 Close the **Group Control** window by clicking in the upper left corner of the **Group Control** window and selecting **Close** from the resulting menu.

- Status updates appear in the **nwadmin** window.
- When the backup is complete, a **Finished** message will appear.

17 If the button for today in step 9 had an **i** on it, go to step 21.

18 Go to the **Customize** menu, select **Schedules**.

- The **Schedules** window opens.

19 Click and hold the button for today, select **Overrides** from the resulting menu, select **Full** from the next resulting menu.

20 Click the **Apply** button.

21 Close the **Schedules** window by clicking in the upper left corner of the **Schedules** window and selecting **Close** from the resulting menu.

22 Select **Exit** from the **File** menu to quit the NetWorker Administrative program.

- The **nwadmin** window closes.

23 At the UNIX prompt for the **machine to be backed up**, type **exit**, then press **Return**.

- **Root** is logged out.

24 Type **exit** again, then press **Return**.

- You are logged out and disconnected from the **machine to be backed up**.

Table 3.3-2 presents the **QUICK STEP** procedure required to perform an incremental backup.

Table 3.3-2. Perform Incremental Backup - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	**ssh** *BackedUpSystemName*	**press Return**
2	*YourPassphrase* **or-** (No entry)	**press Return -or-** (No action)
3	*YourPassword*	**press Return**
4	**su**	**press Return**
5	*RootPassword*	**press Return**
6	**nwadmin**	**press Return**
7	Click Client Click **Client Setup** Click Host Being Backed Up - Highlight the Group to be Backed Up	

8	**Customize → Schedules**	**if i on today's button then go to step 9. Otherwise, click and hold today's button.**
9	**Overrides → Incremental**	**click Apply button**
10	(No entry)	**close Schedules window**
11	(No entry)	**click Group Control button**
12	(No entry)	**click Start button**
12	(No entry)	**click OK button**
14	(No entry)	**close Group Control window**
15	(No entry)	**if there was an i on today's button in step 8, go to step 17.**
16	**Customize → Schedules**	**click and hold today's button**
17	**Overrides → Full**	**click Apply button**
18	(No entry)	**close Schedules window**
19	**File → Exit**	(No action)
20	**exit**	**press Return**
21	**exit**	**press Return**

3.3.2 Full Backup

Non-scheduled full backups can be requested at any time by submitting a for ***Full Backup*** to the OPS supervisor. The supervisor schedules the request with the OPR who performs the full backup. Afterwards, the OPR notifies the requester and supervisor that the full backup is complete.

The **Activity Checklist** table that follows provides an overview of the full backup processes.

Table 3.3-3. Full Backup - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Submit Request for **Full** Backup to OPS Supervisor.	(I) 3.3.2	
2	OPS Super	Schedule Full Backup with **OPR**	(I) 3.3.2	
3	OPR	Perform Full Backup.	(P) 3.3.2	
4	OPR	Notify Requester and OPS Super when Full Backup is Complete.	(I) 3.3.2	

Detailed procedures for tasks performed by the OPR are provided in the sections that follow.

The procedures assume that the requester's application for a full backup has already been approved by DAAC Management. In order to perform the procedure, the OPR must have obtained the following information from the requester:

a. **Name of machine to be backed up**

b. **Files/directories to be backed up** (optional)

To perform a full backup for the requester, execute the procedure steps that follow:

Note 1: If you run out of tapes at any time during this procedure, execute procedure 3.3.5.1 Labeling Tapes and then return to this procedure.

1 Log into the **machine to be backed up** by typing: **ssh *BackedUpSystemName***, then press **Return**.

2 At the Passphrase prompt: enter ***YourPassphrase***, then press **Return**.

- Or press **Return** twice to get to Password prompt.

3 Enter ***YourPassword***, then press **Return.**

- Remember that ***YourPassword*** is case sensitive.
- You are authenticated as yourself and returned to the UNIX prompt.

4 Log in as root by typing: **su**, then press **Return**.

- A password prompt is displayed.

5 Enter the ***RootPassword***, then press **Return**.

- Remember that the ***RootPassword*** is case sensitive.
- You are authenticated as root and returned to the UNIX prompt.

6 Execute the NetWorker Backup program by entering: **nwbackup &**, then press **Return**.

- A **NetWorker Backup** window opens.
- You are now able to perform a full backup.

7 Click Clients.

- Click Client Setup
- Click Host Being Backed Up
- Highlight the group to be Backed Up

8 If no list of **files/directories to be backed up** was provided, i.e. the whole machine is to be backed up, then type **/** in the **Selection** field and click the **Mark** button.

- / is designated for backup and has a check next to it.

9 If names of **files/directories to be backed up** were provided then select the **files/directories to be backed up** in the directory display and click the **Mark** button.

- Drag scroll bar with mouse to scroll the list up and down.
- Double click on directory name to list its contents.
- To move up a directory level, type the path in the **Selection** field.
- Clicking the **Mark** button designates the file for backup and puts a check next to it.

10 Click the **Start** button.

- A **Backup Options** window opens.

11 Click the **OK** button.

- The **Backup Options** window closes.
- The **Backup Status** window opens providing updates on the backup's progress.

12 After the **Backup Completion Time** message appears in the **Backup Status** window, click the **Cancel** button.

- The **Backup Status** window closes.
- The backup is complete.

13 Select **Exit** from the **File** menu to quit the NetWorker Backup program.

- The **NetWorker Backup** window closes.

14 At the UNIX prompt for the **machine to be backed up**, type **exit**, then press **Return**.

- **Root** is logged out.

15 Type **exit** again, then press **Return**.

- You are logged out and disconnected from the **machine to be backed up**.

To perform a full backup, execute the steps provided in the following table.

Table 3.3-4 presents the **QUICK STEP** procedure required to perform a full backup.

Table 3.3-4. Perform Full Backup - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	**ssh** *BackedUpSystemName*	**press Return**
2	*YourPassphrase* **or-** (No entry)	**press Return -or-** (No action)
3	*YourPassword*	**press Return**
4	**su**	**press Return**
5	*RootPassword*	**press Return**
6	**nwbackup &**	**press Return**
7	Click Client Click **Client Setup** Click Host Being Backed Up **-** Highlight the Group to be Backed Up	
8	**to back up whole machine, place / in selection field**	**click Mark button**
9	**to back up certain files/directories, indicate the files/directories**	**click Mark button**
10	(No entry)	**click Start button**
11	(No entry)	**click OK button**
12	(No entry)	**click Cancel button**
13	**File → Exit**	(No action)
14	**exit**	**press Return**
15	**exit**	**press Return**

3.3.3 File Restore

SINGLE OR MULTIPLE FILES RESTORE

From time to time, individual files or groups of files (but not all files) will have to be restored from an Incremental or Full backup tape(s) due to Operator error or system failure. This can be accomplished using the following file restoration procedure.

The File Restore process begins when the requester submits a request to the Operator. The Operator restores the file(s) and notifies the requester when complete.

The Activity Checklist table that follows provides an overview of the file restore process.

Table 3.3-5 File Restore - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Submit Request for File Restore to Operator	(I) 3.3.3	
2	Operator	Restore file(s).	(P) 3.3.3	
3	Operator	Inform Requester of completion.	(I) 3.3.3	
4	Operator	Complete System Restore/Partition Restore	(P) 3.3.3	

Detailed procedures for tasks performed by the Operator are provided in the sections that follow.

The procedures assume that the requester's application for a file restore has already been approved by the Ops Supervisor. In order to perform the procedure, the Operator must have obtained the following information from the requester:

a. **Name of machine to be restored**

b. **Name of file(s) to be restored**

c. **Date from which to restore**

d. **User ID of the owner of the file(s) to be restored**

e. **Choice of action to take when conflicts occur. Choices are:**

- **Rename current file**
- **Keep current file**
- **Write over current file with recovered file**

Table 3.3-6 represents the steps required to restore a file in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed these tasks recently, you should use the detailed procedures presented below.

To restore a file for the requester, execute the procedure steps that follow:

1 Log into the **machine to be restored** by typing: **ssh** , then press **Return**.

2 At the Passphrase prompt: enter ***YourPassphrase***, then press **Return**.

- Or press **Return** twice to get to the Password prompt.

3 Enter ***Your Password***, then press **Return.**

- Remember that your password is case sensitive.
- You are authenticated as yourself and returned to the Unix prompt..

NOTE: Before executing the NetWorker Recovery ensure, that you are in the /data1/COTS/networker directory.

4 Execute the **NetWorker Recovery** program by entering: **nwrecover &**, then press **Return**.

- A window opens for the Networker Recovery program.
- You are now able to perform the file restoration.

5 Select **file(s) to be restored** and click the **Mark** button.

- Drag scroll bar with mouse to scroll the list up and down.
- Double click on directory name to list its contents.
- Clicking the Mark button designates the file for restore and places a check in the box adjacent to the file or directory name.

6 Go to the **Change** menu, select **Browse Time**.

- The Change Browse Time window opens.

7 Select the **date from which to restore**.

- **NetWorker** will automatically go to that day's or a previous day's backup which contains the file.

8 Click the **Start** button.

- The Conflict Resolution window opens.

9 Answer **Do you want to be consulted for conflicts** by clicking the **yes** button, then click the **OK** button.

- If prompted with a conflict, choices of action will be: **rename current file**, **keep current file**, or **write over current file with recovered file**. Select the requesters **choice of action to take when conflicts occur**.
- The Recover Status window opens providing information about the file restore.
- If all the required tapes are not in the drive, a notice will appear. Click the **OK** button in the notice window.
- If prompted for tapes, click cancel in the **Recover Status** window and execute procedure 3.2.5-2 Index Tapes.

10 When a recovery complete message appears, click the **Cancel** button.

11 Go to the **File** menu, select **Exit**.

- The **NetWorker Recovery** program quits.

12 Type **exit**, then press **Return**.

- The **owner of the file(s) to be restored** is logged out.

13 Type **exit** one last time, then press **Return**.

- You are logged out and disconnected from the **machine to be restored.**

To restore a file, execute the steps provided in the following table.

Table 3.3-6. Restore a File - Quick-Step ProceduresÄ

Step	What to Enter or Select	Action to Take
1	**ssh** to the *Machine to be Restored*	**press Return**
2	*Your Passphrase* **-or-** (No entry)	**press Return -or-** (No action)
3	*Your Password*	**press Return**
4	**nwrecover &**	**press Return**
5	**file(s) to be restored**	**click the Mark button**
6	**Change** → **Browse Time**	(No action)
7	**date from which to restore**	**click the Start button**
8	**yes**	**click OK button**
9	(No entry)	**choose what action to take when notified of conflicts**
10	(No entry)	**click Cancel button**
11	**File** → **Exit**	(No action)
12	**exit**	**press Return**
13	**exit**	**press Return**
14	**exit**	**press Return**

3.3.4 Complete System Restore

The Complete System Restore process begins when the requester has determined that a complete system restore is the only way to resolve the problem and has approval from the Operations Supervisor. Once notified of the request, the Operator performs restores of all partitions on the system. Afterwards, the Operator documents and logs all actions in the operator's log book and notifies the requester and Ops Supervisor that the system restore is complete.

The Activity Checklist table that follows provides an overview of the complete system restore process.

Table 3.3-7. Complete System Restore - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Trouble Shoot and Determine that a Complete System Restore is necessary.	(I) 3.3.4	
2	Operator	Restore all Partitions on the System	(P) 3.3.4	
3	Operator	Document and Log in operator's log book, and Inform Requester and Ops Supervisor of completion.	(I) 3.3.4	

Detailed procedures for tasks performed by the Operator are provided in the sections that follow. The procedures assume that the requester's application for a complete system restore has already been approved by Ops Supervisor. In order to perform the procedures, the Operator must have obtained the following information about the requester:

a. **Name of system to be restored**

b. **Date from which to restore**

A complete system restore involves restoring all partitions on that system.

Table 3.2-8 presents the steps required to restore a partition in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed these tasks recently, you should use the detailed procedures presented below.

To restore a partition for the requester, execute the procedures steps that follow:

1 Log into the backup server by typing: **ssh** ***machine to be restored,*** then press **Return**.

2 At the Passphrase prompt: enter ***YourPassphrase***, then press **Return**.

- Or press **Return** twice to get to the Password prompt.

3 Enter ***Your Password***, then press **Return.**

- Remember that ***Your Password*** is case sensitive.
- You are authenticated as yourself and returned to the UNIX prompt.

4 Execute the **NetWorker Administrative** program by entering: **nwadmin &,** then press **Return**.

- A window opens for the NetWorker Administrative program.
- You are now able to perform restores of partitions.

5 Go to the **Save Set** menu, select **Recover Set.**

- The **Save Set Recover** window opens.

6 Select the **Name of system to be restored** (referred to as **System** in the rest of this procedure) in the **Client** field's menu.

- The **Save Set** listing updates. This is a listing of partitions on the **System**.
- At this time, note the partitions listed for the **System**. To do a complete system restore, this procedure needs to be performed for each partition listed.

7 Select the **Save Set**/partition from the listing.

- The **Instance** listing updates.

8 Select the appropriate **Instance**.

- An Instance is a particular Networker client backup. A listing of Instances is a report detailed with the Networker client backups that have occurred.
- Select an Instance based upon the Date from which to restore(referred to as Date in the rest of this procedure) and an appropriate level:

***NOTE** 1: To determine a base **Date**, you must consider the time of day that backups occur. For example, if the backups occur at 02:00 each morning, then a system corrupted at noon on June 6th would require a restoration of the June 6th backup. If the Backups are full or incremental, perform the following actions: Select the most recent full backup that occurred on or prior to the **Date** and perform a partition restore. If the date of this full backup is not the same as the **Date**, perform a partition restore using each incremental backup, in chronological order, between this full backup and the day after the **Date**.

If the backups are of different numerical levels, follow these steps:

1) Select the most recent level **0/full backup** prior to or on the **Date** and perform a restore of the partition.
2) If a level **0/full backup** did not occur on the **Date**, select the most recent backup of the next highest level occurring after this level **0** and prior to or on the **Date**.
3) Perform a restore of the partition.
4) Continue to select the most recent backup of the next highest level occurring between the last used **Instance** and the day after the **Date** until reaching an instance on the **Date**.

- You can double click an **Instance** to see which tape is required.

9 Click the **Recover** button.

- The Save Set Recover Status window opens.
- Clicking the Volumes button will show which tapes are required.

10 Click the **Options** button.

- The **Save Set Recover** Options window opens.

11 Set **Duplicate file resolution** to **Overwrite existing file** by clicking its radio button.

12 Make sure that the **Always prompt** checkbox is not checked.

13 Click the **OK** button.

- The Save Set Recover Options window closes.

14 Click the **Start** button in the **Save Set Recover Status** window.

- Status messages appear in the Status box.
- If prompted for tapes, click the Cancel button in the **Save Set Recover Status** window and follow steps **1-18** of procedure **3.3.5.2** Index tapes(or steps 1-19 of procedures **3.3.5.2** Index Tapes Quick Steps)
- A **recovery complete** message appears when recovery is complete.

15 Click the **Cancel** button after the **recovery complete** message appears.

- The Save Set Recover Status window closes.

16 If additional partition restores are required, go to step **8**. Otherwise, select **Exit** from the **File** menu to quit the NetWorker Administrative program.

17 At the UNIX prompt for the backup server, type **exit**, then press **Return**.

18 Type **exit** again, then press **Return**.

To restore a partition, execute the steps provided in the following table.

Table 3.2-8. Restore a Partition - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	**ssh** ***to the host which requires partition restoration***	**press Return**
2	*Your Passphrase*	**press Return – or -**
3	*Your Password*	**press Return**
4	**nwadmin &**	**press Return**
5	**Save Set → Recover Set**	(no action)
6	**Client/System**	(no action)
7	**Save Set/partition**	(no action)
8	**Instance**	**click Recover button**
9	(No entry)	**click Options button**
10	**Overwrite existing file**	**deselect Always prompt**
11	(No entry)	**click OK button**
12	(No entry)	**click Start button**
13	(No entry)	**click Cancel button**
14	(No entry)	**go to step 7 -or-** **select File → Exit**
15	**exit**	**press Return**
16	**exit**	**press Return**

3.3.5 Tape Handling

The following procedures demonstrate how to label tapes, index tapes, and clean tape drives. Each of these procedures contains detailed steps that explain how to complete the procedure properly. Each tape handling procedure is significant in maintaining a working backup system. DAAC scheduled backups depend on proper maintenance of tape media and tape drives. Listed are complete explanations of the procedures and their relevance to the Computer Operator position.

The Activity Checklist table that follows provides an overview of the tape handling process.

Table 3.3-9. Tape Handling - Activity Checklist

Order	Role	Task	Section	Complete?
1	Operator	Labeling Tapes	(I) 3.3.5.1	
2	Operator	Indexing Tapes	(P) 3.3.5.2	
3	Operator	Tape Drive Cleaning	(P) 3.3.5.3	

3.3.5.1 Labeling Tapes

The Tape Labeling process begins when the Operator is performing procedures 3.3.1 Incremental Backup or 3.3.2 Full Backup (or their associated Quick Steps) and runs out of tapes. The tape(s) must be installed in the jukebox and labeled. NetWorker uses tape labels for identification. The label that NetWorker creates is on the tape media itself, rather than a sticker on the outside of the tape cassette. An index is kept by NetWorker associating tape labels with particular backups/data. When you select files to be recovered using the NetWorker Recovery window or view saved sets on a backup volume using the Volume Management window in NetWorker, you are viewing this index. After labeling the required tape(s), the Operator resumes procedure 3.2.1 or 3.2.2.

Table 3.3-10. Labeling Tapes - Activity Checklist

Order	Role	Task	Section	Complete?
1	Operator	Install Required Tape(s) in Jukebox	(P) 3.3.5.1.1	
2	Operator	Label 8mm Tapes	(P) 3.3.5.1.2	
3	Operator	Label DLT Tapes	(P) 3.4.5.1.3	

Detailed procedures for tasks performed by the Operator are provided in the sections that follow.

3.3.5.1.1 Install Required Tape(s) in Jukebox

The procedures assume that the Operator was previously executing procedure 3.3.1 or 3.3.2. In order to perform the procedures, the Operator must have obtained the following:

a. **Blank tape(s)**

All tapes are stored in the storage cabinet located in the control room. There are five tapes in each box, and every box of tapes has a unique number. To begin finding tapes for recycling to be labeled and installed in the Juke box, the lowest numbers of a tape or a box of tapes should be used. Do not recycle any tape or box of tapes that the numbers are higher or current.

3.3.5.1.2 8mm or D3 Tapes Labeling Process

Table 3.3.5-2 presents the steps required to label tapes in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

To label tapes, execute the procedure steps that follow:

1 Log into the **backup server** by typing: **ssh** ***appropriate server (i.e. gsfcsrvr7)***, then press **Return**.

2 At the Passphrase prompt: enter ***YourPassphrase***, then press **Return**.

- Or press **Return** twice to get to the Password prompt.

3 Enter ***Your Password***, then press **Return**.

- Remember that ***Your Password*** is case sensitive.
- You are authenticated as yourself and returned to the UNIX prompt.

4 Execute the **NetWorker Administrative** program windows by entering: **nwadmin &**, then press **Return**.

- The **NetWorker Administrative** program windows displayed
- Remove all non-blank tapes from the cartridge.
- ***Dismount the drive(s) that will be used for tapes Labeling***

5 Insert the blank tape(s) in the jukebox's cartridge, then install the cartridge in the jukebox.

6 Click the **Label** button from the menu bar.

- The **Jukebox Labeling** window opens.

7 Enter **tape one** in the non-removable **Slot field**.

- **Slot 1** is at the top of the cartridge, and it is a non-removable slot. **Slot 2** through **Slot 11** are removable slots. **Slot 11** contains a cleaning tape. Do not enter any tape in Slot 11 for labeling. The default setting is **1** through **10** for only the tapes that will be labeled and used for backup.
- It is ok to have empty slots.

8 Click the **OK** button.

- A status message appears and updates.
- Labeling a full cartridge of tapes takes about one and half hours. Nine Minutes per tape.

9 When the status in the **Jukebox Labeling** window reads finished, click the **Cancel** button.

- The **Jukebox Labeling** window closes.

10 Go to the **File** menu, select **Exit**.

11 Put a sticker on the outside of each tape cassette.

- This is done in order for you to identify each tape.

11 Resume procedure 3.3.1 or 3.3.2.

To label tapes, execute the steps provided in the following table.

3.3.5.1.3 Label DLT Tapes

The dlt tape labeling process is the same as the 8mm tape labeling scenarios, except for some few things that are additionally different. Steps to follow in labeling the dlt tapes as follow: Repeat Table **3.3.5.1** step 1 through step 9. Change default to **SPRDLT,** then click OK button. The system will display the beginning number of the tape label. Once again repeat step 11 through step 17 of Table **3.3.5.1**, tape labeling process to end the task.

Table 3.3-11. Label Tapes - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	**ssh***to* ***appropriate server (i.e. gsfcsrvr7)***	**press Return**
2	*Your*Passphrase	**press Return – or -**
3	*Your Password*	**press Return**
4	No Entry	**press Return**
5	**nwadmin &**	**press Return**
6	(No entry)	**put blank tape(s) in cartridge and install cartridge in jukebox**
7	(No entry)	**click Label button**
8	**2**	(No action)
9	**11**	**click OK button**
10	(No entry)	**click Cancel button**
11	**File → Exit**	(No action)
12	**exit**	**press Return**
13	**exit**	**press Return**
14	(No entry)	**put a sticker on the outside of each tape**
15	(No entry)	**resume previous procedure**

3.3.5.2 Indexing Tapes

The Indexing Tapes process begins when the Operator has finished performing procedures 3.3.5.1, (**Tape Labeling**). If the tape(s) is/are not ***indexed/inventoried,*** Networker will not be aware of it/them. After indexing the required tape(s), the Operator resumes procedure 3.3.1 or 3.3.2.

The Activity Checklist table that follows provides an overview of the indexing tapes process.

Table 3.3-12. Indexing Tapes - Activity Checklist

Order	Role	Task	Section	Complete?
1	Operator	Pull Required Tape(s) from Tape Storage.	(I) 3.3.5.2.1	
2	Operator	Index Tapes	(P) 3.3.5.2.2	

3.3.5.2.1 Pull Required Tape(s) from Tape Storage

In order to perform the procedure, the Operator must have obtained the following:

a. **The required tape(s)**

3.3.5-2 Index Tapes

Detailed procedures for tasks performed by the Operator are provided in the sections that follow.

The procedures assume that the Operator has previously executed procedure 3.3.5.1, **Tape Labeling**.

Table **3.3-5-2** presents the steps required to index tapes in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

To index tapes, execute the procedure steps that follow:

NOTE: You may proceed to step **8** if you are still logged into the backupserver.

1 Log into the **backup server** by typing: **ssh** ***appropriate server (i.e. gsfcsrvr7),*** then press **Return**.

2 At the Passphrase prompt: enter ***YourPassphrase***, then press **Return**.

- Or press **Return** twice to get to the Password prompt.

3 Enter ***Your Password***, then press **Return.**

- Remember that your password is case sensitive.
- You are authenticated as yourself and returned to the Unix prompt.

4 Execute the **Networker Administrative** program by entering: **nwadmin &,** then press **Return**.

- The Networker Administrative program windows is displayed.
- You are now able to index tapes.
- Click the Mount button to show what tapes **Networker** is currently aware of. The **Jukebox Mounting** windows opens. Once you have finished with this window, click the **Cancel** button.

5 Put the **required tape(s)** in the jukebox's cartridge, install the cartridge in the jukebox.

- For instructions, refer to the jukebox's documentation.

6 Go to the **Media** menu, select **Inventory**.

- The **Jukebox Inventory** window opens.

7 Enter **1** in the **First Slot** field, enter **10** in the **Last Slot** field.

- Slot 1 is the non-removable slot within the jukebox.
- Slot 2 is the first top of the removable cartridge and 11 at the bottom, and it contains a cleaning tape. A default setting 1 through 10.
- It is OK to have empty slots or slots with tapes which have already been indexed.

8 Click the **OK** button.

- A checking volume message appears and updates.
- Performing an inventory on a full cartridge takes about forty minutes.

9 When the status in the **Jukebox Inventory** window says finished, click the **Cancel** button.

- The **Jukebox Inventory** window closes.

10 Click the **Mount** button to verify that the indexing worked.

- The Jukebox Mounting window opens.
- The required tape(s) should be shown. If not, repeat from step 8.

11 Click the **Cancel** button.

- The **Jukebox Mounting** window closes.

12 Go to the **File** menu, select **Exit**.

13 At the UNIX prompt for the ***backup server***, type **exit**, then press **Return**.

14 Type **exit** again, then press **Return**.

15 Resume procedure 3.3.3 at step 12, procedure 3.3.3 at quick-step 11 - action part, procedure 3.3.4 at step 12, or procedure 3.3.4 at quick-step 11 - action part.

To index tapes, execute the steps provided in the table.

Table 3.3-12. Index Tapes - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	**ssh** ***appropriate server (i.e. gsfcsrvr7)***	**press Return**
2	*Your Passphrase*	**press Return - or -**
3	*Your Password*	**press Return**
4	**nwadmin**	**press Return**
5	(No entry)	**put required tape(s) in cartridge and install cartridge in jukebox**

6	**Media → Inventory**	(No action)
7	**2**	(No action)
8	**11**	**click OK button**
9	(No entry)	**click Cancel button**
10	(No entry)	**click Mount button**
11	(No entry)	**verify indexing**
12	(No entry)	**click Cancel button**
13	**File → Exit**	(No action)
14	**exit**	**press Return**
15	**exit**	**press Return**
16	(No entry)	**resume previous procedure**

3.3.5.3 Tape Cleaning Process

The system will at times prompt for drive(s) cleaning. This happens usually during non processing periods, however during the course of the tape backup process period, the drive(s) may send a request for cleaning. Manual cleaning should be performed each time tapes are installed in the Juke Box. Maintaining clean drives can help prevent backup interruption which may occur due to unclean tape drive heads. If the system is prompted for drive(s) cleaning: Follow the details steps below:

(1) Log into the Backup Server by typing: **ssh *appropriate server (i.e. gsfcsrvr7)***, then press **Return.**

- The system prompts for your Passphrase

(2) Type yourPassphrase, then press **Return.**

- Or press **Return** twice to get to the Password prompt.

(3) Type your **password,** then press **Return.** Remember, your password is case sensitive.

(4) Execute Net Worker by typing: **nwadmin &**, then press Return.

- A NetWorker administrative program windows displayed.

(5) Highlight the desirable drive(s) that the system has prompted for cleaning.

(6) Click dismount from the menu bar and wait a few minutes for the drive to be dismounted completely. Repeat step 6 on the second drive until the both are dismounted.

To open the Exabyte door turn the key in the door counter clockwise. The last tape at the bottom of the cartridge is the cleaning tape. Remove it from the slot field and insert it gently into each drive below. Wait until the tape has been ejected and the flashing lights on the drive are off before removing the tape from the drive. Insure that the cleaning tape is still usable before each use. Cleaning tapes will expire after several uses. After each use mark the appropriate box on the surface of the tape to maintain a list of usage. Insert the cleaning tape back into the last slot and lock the Exabyte door.

1. 3.4 User Administration

Note: User Administration procedures will be implemented through command-line and/or script entries. The Tivoli Management Environment (TME) will not be used for User Administration procedures.

3.4.1 Adding a User

The Adding a User process begins when the requester fills out a "User Registration Request Form" (located in Appendix A), and submits it to the site supervisor. The "User Registration Request Form" includes information regarding the user (User’s Name, Group, Organization, etc.), as well as the user's explanation of why an account on the system is needed. The requester's supervisor reviews the request, and if it is determined that it is appropriate for the requester to have UNIX and DCE accounts, forwards the request to the Operations Supervisor (OPS Super). The OPS Super reviews the request and forwards it to the System Administrator (SA). The SA verifies that all required information is contained on the form. If it is, the SA implements the request. (Incomplete forms are returned to the requester’s supervisor for additional information.) After the user is registered, the SA provides the user with a password to use for logging onto their accounts. The SA also sends an e-mail message to the user's supervisor and the OPS Super, informing them that the user's accounts were created.

The **Activity Checklist** table that follows provides an overview of the adding a user process.

Table 3.4-1. Adding a User - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Complete User Registration Form and forward to the Supervisor.	(I) 3.4.1	
2	Super	Approve/Deny Request. If Approve, Forward Request to OPS Super.	(I) 3.4.1	
3	OPS Super	Review Request and Forward to SA.	(I) 3.4.1	
4	SA	Review User Registration Form for Completeness.	(I) 3.4.1	
5	SA	Add User.	(P) 3.4.1	
6	SA	Phone/e-mail User with Password. Notify Supervisor and OPS Super that user was added.	(I) 3.4.1	

Depending upon the script utilized, in order to add a new user the SA should obtain information such as the following about the requester:

a. **Real name of the new user**

b. **User name of the new user**

c. **Office number of the new user**

d. **Office phone number of the new user**

e. **Home phone number of the new user**

f. **Organization**

g. **Group affiliation(s)**

h. **Role(s) of the new user**

The SA creates a new user account with command-line/script entries. As an example, The Goddard Space Flight Center DAAC uses a script, *Newuser*, to add new users to the system. The script, which is available to other DAACs, walks the System Administrator through data input of user information, checks for the same user in other systems, creates a User ID, synchronizes password files and creates home directories for new users.

3.4.2 Deleting a User

The Deleting a User process begins when the requester has determined that no useful files remain in the user’s home directory and submits a request to delete the user’s account to the user’s supervisor. The supervisor approves or denies the request. Once approved, the request is forwarded to the OPS Super. The OPS Supervisor reviews the request and forwards it to the SA, who deletes the user's account. When the user has been deleted, the SA notifies the requester, supervisor and OPS Super.

The Activity Checklist table that follows provides an overview of the deleting a user account process.

Table 3.4-2. Deleting a User - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Determine that No Useful Files Remain in the User's Home Directory and Submit Request to user's Supervisor.	(I) 3.4.2	
2	OPS Super	Approve/Deny Request. If Approve, Forward Request to OPS Super.	(I) 3.4.2	
3	OPS Super	Review Request and Forward to SA.	(I) 3.4.2	
4	SA	Delete User.	(P) 3.4.2	
5	SA	Notify Requester, Supervisor and OPS Super that user was deleted.	(I) 3.4.2	

The process assumes that the requester's application for deleting a user has already been approved by DAAC Management. In order to perform the procedure, the SA must have obtained the following information from the requester:

a. **UNIX login of the user to be deleted**

a. **Role(s) of the user to be deleted**

The SA deletes a user with command-line/script entries. As an example, The Goddard Space Flight Center DAAC uses a script, *Lockdown,* to lock, unlock and delete user accounts. This script, which is available to other DAACs, walks the System Administrator through the steps necessary to delete a user account. It assists the System Administrator in locating the correct user account for deletion, deletes the user account and all associated file references. It also enables the System Administrator to lock or unlock accounts.

3.4.3 Changing a User Account Configuration

The Changing a User Account Configuration process begins when the requester submits a request to the OPS Supervisor detailing what to change about the account configuration and the reason for the change. The OPS Supervisor reviews the request and forwards it to SA who changes the user's account configuration. When the changes are complete the SA notifies the requester and OPS Supervisor.

The Activity Checklist table that follows provides an overview of the changing a user account configuration process.

Table 3.4-3. Change a User Account Configuration - Activity Checklist

Order	Role	Task	Section	Complete ?
1	Requester	Submit Request to OPS Supervisor.	(I) 3.4.3	
2	OPS Super	Review and Forward to SA.	(I) 3.4.3	
3	SA	Change User Account Configuration.	(P) 3.4.3	
4	SA	Inform Requester and Supervisor of completion.	(I) 3.4.3	

The process assumes that the requester's application for changing a user account configuration has already been approved by the OPS Supervisor. In order to perform the procedure, the SA must have obtained the following information from the requester:

a. **What to change and new settings.**

Can be any of:

New Real User Name

New Login ID

New Office Number

New Office Phone Number

New Home Phone Number

New UNIX Group

New DCE Group

New DCE Organization

New Login Shell

b. **Current UNIX Login of the User**

The SA changes the appropriate configuration items manually in the users home directory.

3.4.4 Changing User Access Privileges

The Changing User Access Privileges process begins when the requester submits a request to the supervisor. The supervisor approves or denies the request. Once approved, the request is forwarded to the OPS Super. The OPS Super reviews the request and forwards it to the SA who changes the user's access privileges. When the changes are complete the SA notifies the requester, supervisor and OPS Super.

The Activity Checklist table that follows provides an overview of the changing user access privileges process.

Table 3.4-7. Changing User Access Privileges - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Submit Request to the Supervisor.	(I) 3.4.4	
2	Super	Approve/Deny Request. If Approve, Forward Request to OPS Super.	(I) 3.4.4	
3	OPS Super	Review Request and Forward to SA.	(I) 3.4.4	
4	SA	Change User Access Privileges.	(P) 3.4.4	
5	SA	Inform Requester, Supervisor and DAAC Mgr of completion.	(I) 3.4.4	

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the requester's application for changing user access privileges has already been approved by DAAC Management and that the SA is an administrator. In order to perform the procedure, the SA must have obtained the following information about the requester:

a. **Role(s) to which the user is to be added**

b. **Role(s) from which the user is to be removed**

c. **UNIX login of the user**

To change user access privileges for the requester, execute the procedure steps that follow:

3.4.5 Changing a User Password

The Changing a User Password process begins when the requester submits a request to the SA. The SA verifies that the requester is who s/he claims to be. Once verified, the SA changes the user's password. When the change is complete the SA notifies the requester.

The **Activity Checklist** table that follows provides an overview of the changing a user password process.

Table 3.4-9. Changing a User Password - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Submit Request to SA.	(I) 3.4.5	
2	SA	Verify that the Requester is Who S/he Claims to Be.	(I) 3.4.5	
3	SA	Change Password.	(P) 3.4.5	
4	SA	Inform Requester of completion.	(I) 3.4.5	

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the requester's application for changing a user password has already been approved by DAAC Management and that the SA is a Tivoli administrator. In order to perform the procedure, the SA must have obtained the following information about the requester:

a. **UNIX login of the user**

b. **New password for the user**

To change a user password for the requester, execute the procedure steps that follow:

3.4.6 Checking a File/Directory Access Privilege Status

The Checking a File/Directory Access Privilege Status process begins when the requester submits a request to the SA. The SA checks the file/directory access privilege status and reports the status back to the requester.

The **Activity Checklist** Table 3.4-11 that follows provides an overview of the checking a file/directory access privilege status process.

Table 3.4-11. Checking a File/Directory Access Privilege Status - Activity Checklist

Order	Role	Task	Section	Complete ?
1	Requester	Submit a Request to the SA.	(I) 3.4.6	
2	SA	Check a File/Directory Access Privilege Status.	(P) 3.4.6	
3	SA	Inform Requester of completion and Report the File/Directory Access Privilege Status.	(I) 3.4.6	

Detailed procedures for tasks performed by the SA are provided in the sections that follow. In order to perform the procedure, the SA must have obtained the following information about the requester:

a. **full path of the file/directory on which privilege status is needed**

Table 3.4-12 contains a table which presents the steps required to check a file/directory access privilege status in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

To check a file/directory access privilege status for the requester, execute the procedure steps that follow:

1 At a UNIX prompt, type **cd *Path***, press **Return**.

- The ***Path*** is the full path up to but not including the file/directory on which access privilege status is needed. For example, if the requester wants access privileges status on directory /home/jdoe then type **cd /home** and press **Return**.

2 Type **ls -la | grep *FileOrDirectoryName***, press **Return**.

This command will return information like this:

```
drwxr-xr-x  19 jdoe user    4096 Jun 28 09:51 jdoe
-r-xr--r--   1  jdoe user     80   Jun 22 11:22 junk
```

What this output means, from left to right, is:

The file type and access permissions:

The *first character* indicates what type of file it is:
d means that the file is a directory.
- means that the file is an ordinary file.
l means that the file is a symbolic link.

The *next three characters* indicate the owner privileges, in the order: **r** = read **w** = write **x** = execute. **-** is a place holder. ***Example:*** the owner (jdoe) of the file ***junk*** does not have *write* permissions, so a - appears rather than a w.

The *next three characters* indicate the group privileges, in the order: **r** = read **w** = write **x** = execute. **-** is a place holder. ***Example:*** the group (user) of the directory ***jdoe*** does not have write permissions, so a - appears rather than a w as the sixth character in the line.

The *next three characters* indicate the privileges that everyone else/other has, in the order: **r** = read **w** = write **x** = execute. **-** is a place holder. ***Example:*** other in the case of the directory ***jdoe*** does not have write permissions, so a - appears rather than a w as the ninth character in the line.

There are 19 links to the file/directory ***jdoe***.
The owner of the file/directory is jdoe.
The file/directory's group is user.
The file/directory is 4096 bytes large.
The last time the file/directory was modified is Jun 28 at 09:51.
The name of the file/directory is jdoe.

3 Create a report of the file/directory's access privilege status by using the information produced by step 2 and by filling out this template:

full path of the file/directory: ____

owner: ____

group: ____

owner/user privileges: ______ **read** _______ **write** _______ **execute**

group privileges: _______ **read** _______ **write** _______ **execute**

everyone else/other privileges: _______ **read** _______ **write** _______ **execute**

To check a file/directory access privilege status, execute the steps provided in the following table.

Table 3.4-12. Check a File/Directory Access Privilege Status - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	**cd *Path***	**press Return**
2	**ls -la | grep *FileOrDirectoryName***	**press Return**

3	(No entry)	**generate a file/directory access privilege status report**

3.4.7 Changing a File/Directory Access Privilege

The Changing a File/Directory Access Privilege process begins when the requester submits a request to the supervisor to have file/directory access privileges changed. The supervisor approves/denies the request. When approved, the request is forwarded to the OPS Supervisor who reviews the request and forwards it to the SA. The SA changes the file/directory access privileges and then notifies the requester, supervisor and OPS Supervisor of completion.

The **Activity Checklist** table that follows provides an overview of the changing a file/directory access privilege process.

Table 3.4-13. Changing a File/Directory Access Privilege - Activity Checklist

Order	Role	Task	Section	Complete ?
1	Requester	Submit Request to the Supervisor.	(I) 3.4.7	
2	Super	Approve/Deny Request. If Approve, Forward Request to OPS Supervisor.	(I) 3.4.7	
3	OPS Super	Review Request and Forward to SA.	(I) 3.4.7	
4	SA	Change a File/Directory Access Privilege.	(P) 3.4.7	
5	SA	Inform Requester, Supervisor and OPS Supervisor of completion.	(I) 3.4.7	

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the requester's application for changing a file/directory access privilege has already been approved by the supervisor. In order to perform the procedure, the SA must have obtained the following information about the requester:

a. **full path of the file/directory on which access privileges will be changed**

b. **new access privileges to set on the file/directory. Can be any of:**

New owner

New group

New user/owner privileges (read, write and/or execute)

New group privileges (read, write and/or execute)

New other privileges (read, write and/or execute)

To change a file/directory access privilege for the requester, execute the procedure steps that follow:

1 At the UNIX prompt, type **su**, press **Return**.

2 At the **Password** prompt, type ***RootPassword***, press **Return**.

- Remember that ***RootPassword*** is case sensitive.
- You are authenticated as root.

3 Type **cd *Path***, press **Return**.

- The ***Path*** is the full path up to but not including the file/directory on which access privileges will be changed. For example, if the requester wants access privileges changed on directory /home/jdoe then type **cd /home** and press **Return**.

4 If there is a **New owner** then type **chown *NewOwner FileOrDirectoryName***, press **Return**.

- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe then type: (You must be /home)
  chown *NewOwner* jdoe and press **Return**.

5 If there is a **New group** then type **chgrp *NewGroup FileOrDirectoryName***, press **Return**.

- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe then type:
  chgrp *NewGroup* jdoe and press **Return**.

6 If there are **New user/owner privileges** then type **chmod u=*NewUserPrivileges FileOrDirectoryName***, press **Return**.

- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe then type:
  chmod u=*NewUserPrivileges* jdoe and press **Return**.

- The ***NewUserPrivileges*** are **r** = read **w** = write **x** = execute. To give the user/owner read, write and execute privileges, type:
  chmod u=rwx *FileOrDirectoryName* and press **Return**.

7 If there are **New group privileges** then type **chmod g=*NewGroupPrivileges FileOrDirectoryName***, press **Return**.

- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. ***Example:*** if the requester wants access privileges changed on directory /home/jdoe then type: (You must be in /home)
  chmod g=*NewGroupPrivileges* jdoe and press **Return**.

- The ***NewGroupPrivileges*** are **r** = read **w** = write **x** = execute.
  Example: to give the group read and execute privileges, type:
  chmod g=rx *FileOrDirectoryName* and press **Return**.

8 If there are **New other privileges** then **type:**
chmod o=*NewOtherPrivileges* *FileOrDirectoryName*, and press **Return**.

- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe then type:
  chmod o=*NewOtherPrivileges* jdoe, and press **Return**.

- The ***NewOtherPrivileges*** are r for read, w for write and x for execute. For example, to give other read privileges, type:
  chmod o=r *FileOrDirectoryName* and press **Return**.

9 Type **exit**, press **Return**.

- Root is logged out.

To change a file/directory access privilege, execute the steps provided in the following table.

Table 3.4-14 contains a table which presents the steps required change a file/directory access privilege.

Table 3.4-14. Change a File/Directory Access Privilege - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	su	press Return
2	*RootPassword*	press Return
3	cd *Path*	press Return
4	chown *NewOwner FileOrDirectoryName*	press Return
5	chgrp *NewGroup FileOrDirectoryName*	press Return
6	chmod u=*NewUserPrivileges FileOrDirectoryName*	press Return
7	chmod g=*NewGroupPrivileges FileOrDirectoryName*	press Return
8	chmod o=*NewOtherPrivileges FileOrDirectoryName*	press Return
9	exit	press Return

3.4.8 Moving a User's Home Directory

The Moving a User's Home Directory process begins when the requester submits a request to the OPS Supervisor. The OPS Supervisor approves or denies the request. Once approved, the request is forwarded to the SA who moves the user's home directory. When the changes are complete the SA notifies the requester and OPS Supervisor.

The Activity Checklist table that follows provides an overview of moving a user's home directory process.

Table 3.4-15. Moving a User's Home Directory - Activity Checklist

Order	Role	Task	Section	Complete ?
1	Requester	Submit Request to OPS Supervisor.	(I) 3.4.8	
2	OPS Super	Approve/Deny Request in Accordance with Policy. Forward to SA if approved.	(I) 3.4.8	
3	SA	Move a User's Home Directory.	(P) 3.4.8	
4	SA	Inform Requester and OPS Super of completion.	(I) 3.4.8	

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the requester's application for moving a user's home directory has already been approved by DAAC Management and that the SA is an administrator. In order to perform the procedure, the SA must have obtained the following information about the requester:

a. **UNIX login of the user**

b. **New location for home directory**

To move a user's home directory for the requester, execute the procedure steps that follow:

3.5 Installing a New Workstation

The Installing a New Workstation process has three stages - preparation, installation and testing, and verification. The preparation stage begins with the System Administrator (SA) performing procedure 3.5.1.1 Hardware Preparation. Once the hardware is prepared, the SA continues on and prepares for network configuration, procedure 3.5.1.2.

The next stage is installation which begins by reporting the hardware to inventory, procedure 3.5.2.1.1. The SA continues this stage by installing the operating system, procedure 3.5.2.2. Installation is then completed by installing custom software, procedure 3.5.2.3.1, and installing COTS software, procedure 3.5.2.3.2.

The final stage is testing and verification. The SA begins this stage by rebooting the machine, procedure 3.5.3.1. The testing and verification is completed by logging in, procedure 3.5.3.2, and testing the environment, procedure 3.5.3.3.

The Activity Checklist table that follows provides an overview of the New Workstation Installation process.

Table 3.5-1. Installing a New Workstation - Activity Checklist

Order	Role	Task	Section	Complete?
1	SA	Prepare Hardware	(P) 3.5.1.1	
2	SA	Prepare for Network Configuration	(P) 3.5.1.2	
3	SA	Report Hardware to Inventory	(P) 3.5.2.1.1	
4	SA	Install Operating System	(P) 3.5.2.2	
5	SA	Install Custom Software	(P) 3.5.2.3.1	
6	SA	Install COTS Software	(P) 3.5.2.3.2	
7	SA	Reboot	(P) 3.5.3.1	
8	SA	Log In	(P) 3.5.3.2	
9	SA	Test Environment	(P) 3.5.3.3	

3.5.1 Preparation

3.5.1.1 Hardware Preparation

The Hardware Preparation process begins when the requester submits a request to the SA. The SA then determines if the requested hardware is on hand or must be ordered. Once the hardware is available along with all the necessary attachments, the SA will schedule the installation. After the Hardware Preparation is complete, the SA proceeds to procedure 3.5.1.2, Network Configuration.

The Activity Checklist table that follows provides an overview of the Hardware Preparation process.

Table 3.5-2. Hardware Preparation - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Make request known to Operation Supervisor	(I) 3.5.1.1	
2	OPS Super	Submit a request to the DAAC Manager for approval	(I) 3.5.1.1	
3	DAAC Manager	Submit approved request to the SA	(I) 3.5.1.1	
4	SA	Determine if the requested hardware is on hand or must be ordered. Network is in place and IP Addresses have been assigned to hardware.	(I) 3.5.1.1	
5	SA	Schedule the Installation.	(I) 3.5.1.1	

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the hardware installation has been scheduled well in advance, all planning involved has been concluded well in advance and the SA has been properly trained to install the hardware. The SA must obtain the following information from the requester:

a. **type of hardware desired (HP, Sun, SGI or NCD)**

b. **location of installation**

Refer to Section 3.3 of the Release A Installation Plan (800-TP-005-001) for detailed instruction on how to install hardware.

3.5.1.2 Network Configuration

The Network Configuration process begins after section 3.5.1.1 Hardware Preparation has been completed in the Installing a New Workstation process. Once complete, the SA proceeds to procedure 3.5.2.1.1 Reporting to Inventory.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that procedure 3.5.1.1 Hardware Preparation has been completed and that the SA has been properly trained in network configuration.

The following steps are required to prepare for network configuration:

1 Determine the name of the hardware.

- For example, if the hardware is a NCD, the name will be ncd# where # is sequential from the inventory list. The standard naming convention follows: (ex. g0css02)
- x = DAAC site (i.e., g = goodard, l = langley, e = edc, n = nsidc)
- 0 = B0 machine
- c = characters for subsystem identification
- s = characters for subsystem identification
- s = machine type (i.e., s = sun, g = sgi, h = hp)
- 0x = x indicates the number of machines in that subsystem suite (?) (i.e., 01, 02, etc)

NOTE: If the hardware is a NCD, the SA needs to determine the name of the NCD Login Host. The NCD Login Host will be the name of the X-server this NCD will use.

2 Submit a request to the Resource Manager for the IP address and the DNS entry.

To prepare for network configuration, execute the steps provided in the following table.

Table 3.5-3 presents the **QUICK STEP** procedures required to prepare for network configuration.

Table 3.5-3. Prepare for Network Configuration - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	**determine name of workstation**
2	(No entry)	**determine NCD Login Host**
3	(No entry)	**submit request to Resource Manager for IP address and DNS entry**

3.5.2 Installation

3.5.2.1 Hardware

3.5.2.1.1 Reporting to Inventory

The Reporting to Inventory process begins after the SA has completed Section 3.5.1.1 Hardware Preparation and 3.5.1.2 Network Configuration. After the Reporting to Inventory is complete, the SA proceeds to procedure 3.5.2.2 Operating System Installation.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that procedures 3.5.1.1 and 3.5.1.2 have been completed.

The following steps are required to report to inventory:

1 Locate the Inventory Control Number on each hardware component and record them.

- The Inventory Control Number is on a small bright sticker on the front of each hardware component.

2 Submit the Inventory Control Numbers and location of the machine to the Inventory Controller.

To report to inventory, execute the steps provided in the following table.

Table 3.5-4 presents the **QUICK STEP** procedures required to report to inventory.

Table 3.5-4. Report to Inventory - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	**locate and record the Inventory Control Numbers**
2	(No entry)	**report the Inventory Control Numbers and location of the machine to the Inventory Controller**

3.5.2.2 Operating System Installation - By Operating System Type

3.5.2.2.1 Solaris 2.5.1 Operating System Installation

Solaris 2.5.1 is also known as Sun OS 5.5.1. The Solaris 2.5.1 Operating System Installation process begins when procedure 3.5.2.1 Installation of Hardware has been completed in the Installing a New Workstation process. Once complete, the SA proceeds to procedure 3.5.2.3.1 Installation of Custom Software.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedure assumes that procedures 3.5.1 Preparation and 3.5.2.1 Installation of Hardware have been completed. The procedure also assumes that the workstation is powered off.

This section explains how to install the Solaris 2.5.1 operating system, including network configuration and patch installation. If you would like a listing of the patches installed, please see document number 420-TD-012-001 Release A Sun Solaris Operating System Patch List attached at the end of this document. To install the Solaris 2.5.1 operating system, execute the procedure steps that follow:

1 Get the download disk.

2 Check that the download disk is set to be target 2.

- Facing the front of the download disk, the target number is found on the back, to the right on the disk.
- You can change the target number by hitting the pins above and below it.

3 Plug the download disk into the Sun.

4 Power on the download disk.

- Facing the front of the disk, the power switch is found on the back, to the left on the disk.

5 Power on the monitor, power on the Sun.

- The Sun's power switch is located on the back of the Sun. When facing the front of the Sun, the power switch is on the right.

6 At the > prompt, type **probe-scsi**, press **Return**.

- Verify that target 2 exists by finding it in the listing that appears.

7 Type **boot disk2 -swr**, press **Return**.

- The Sun boots up.
- s is for single user, w is for writeable and r is for reconfigure (required because you added a drive).

8 Type ***RootPassword***, press **Return**.

- ***RootPassword*** is the root password for the download disk.
- Remember that the ***RootPassword*** is case sensitive.
- You are authenticated as root and returned the UNIX prompt.

9 Type **/download/setup**, press **Return**.

- Status messages will be displayed.

10 When prompted for the Sun's name, type ***SunsName***, press **Return**.

11 When prompted for the Sun's IP address, type ***SunsIP***, press **Return**.

- The Sun's network and hostname are configured.

12 When you are returned to a UNIX prompt, type **/etc/halt**, press **Return**.

13 At the > prompt, power off the download disk.

14 Disconnect the download disk from the Sun.

15 At the > prompt, type **boot -r**, press **Return**.

- The Sun boots up.
- r is for reconfigure (required because you removed a drive).

16 At the **login:** prompt, type **root**, press **Return**.

17 Type ***RootPassword***, press **Return**.

- ***RootPassword*** is the root password for the download disk. (The Sun uses the download disk's root password until a new one is set.)
- Remember that the ***RootPassword*** is case sensitive.
- You are authenticated as root and returned the UNIX prompt.

18 Type **passwd root**, press **Return**.

19 At the **New password:** prompt, type ***RootPassword***, press **Return**.

- ***RootPassword*** is the root password for the Sun.
- Remember that the ***RootPassword*** is case sensitive.

20 At the **Re-enter new password:** prompt, type ***RootPassword***, press **Return**.

- ***RootPassword*** is the root password for the Sun.

- This step confirms that the root password has been entered correctly.
- Remember that the ***RootPassword*** is case sensitive.
- The root password for this Sun is set. Inform all authorized personnel of ***RootPassword***.

21 Type **exit**, press **Return**.

- Root is logged out of the Sun.

22 Inform the backup administrator of the new machine.

To install the Solaris 2.5.1 operating system, execute the steps provided in the following table.

Table 3.5-5 presents the **QUICK STEP** procedures required to install the Solaris 2.5.1 operating system.

Table 3.5-5. Install the Solaris 2.5.1 Operating System - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	**get the download disk**
2	(No entry)	**check that download disk is set to target 2**
3	(No entry)	**plug download disk into Sun**
4	(No entry)	**power on download disk**
5	(No entry)	**power on monitor**
6	(No entry)	**power on Sun**
7	probe-scsi	**press Return**
8	(No entry)	**verify that target 2 exists**
9	boot disk2 -swr	**press Return**
10	*RootPassword of download disk*	**press Return**
11	/download/setup	**press Return**
12	*SunsName*	**press Return**
14	*SunsIP*	**press Return**
15	/etc/halt	**press Return**
16	(No entry)	**power off download disk**
17	(No entry)	**disconnect download disk from Sun**
18	boot -r	**press Return**
19	root	**press Return**
20	*RootPassword of download disk*	**press Return**
21	passwd root	**press Return**
22	*RootPassword for the Sun*	**press Return**
23	*RootPassword for the Sun*	**press Return**
24	exit	**press Return**
25	(No entry)	**inform all authorized personnel of *RootPassword for the Sun***
26	(No entry)	**inform backup administrator of new Sun**

3.5.2.2.2 HP-UX 10.01 AND 10.10 Operating System Installation

The HP-UX 10.01 and 10.10 Operating System Installation process begins when procedure 3.5.2.1 Installation of Hardware has been completed in the Installing a New Workstation process. Once complete, the SA proceeds to procedure 3.5.2.3.1 Installation of Custom Software.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedure assumes that procedures 3.5.1 Preparation and 3.5.2.1 Installation of Hardware have been completed. The procedure also assumes that the workstation is powered off.

This section explains how to install the HP-UX 10.01 and 10.10 operating system, including network configuration and patch installation. If you would like a listing of the patches installed, please see document number 420-TD-014-001 Release A HP Operating System Patch List attached at the end of this document. To install the HP-UX 10.01 and 10.10 operating system, execute the procedure steps that follow:

1 Get the download disk.

2 Check that it is set to be target 2.
- The target number is found on the back of the disk.
- You can change the target number by hitting the buttons above and below it.

3 Plug the download disk into the HP.

4 Power on the download disk.
- The power switch is located on the back of the drive.

5 Power on the monitor, power on the HP.
- The power switch is located on the right side of the HP, towards the front.
- The HP starts booting up.

6 At the **Selecting a system to boot. To stop selection process press and hold the ESCAPE key** message, press and hold **Escape**.
- You have 10 seconds to press **Escape** before the boot process proceeds.
- The boot process will stop and a menu of boot commands will appear.

7 Select boot scsi.2.0 by typing **b *DeviceSelectionForscsi.2.0* isl**, press **Return**.
- For example, if the Device Selection for scsi.2.0 in the menu is P1 then type **b P1 isl** and then press **Return.**
- **isl** will cause the HP to boot in interactive mode.

8 At the **ISL>** prompt, type **hpux -is boot disk(scsi.2;0)/hp-ux**, press **Return**.
- **-is** causes the HP to boot in single user mode.
- You will be returned to the UNIX prompt.

9 Type **/download/setup**, press **Return**.
- Status messages will be displayed.

10 When prompted for the HP's name, type ***HPsName***, press **Return**.

11 When prompted for the HP's IP address, type ***HPsIP***, press **Return**.
- The HP's network and hostname are configured.

12 When you are returned to a UNIX prompt, type **/etc/shutdown -h -y now**, press **Return**.
- The HP shuts down and comes to a halt.

13 Once the HP has halted, power off the download disk, power off the monitor.

14 Power off the HP.

15 Disconnect the download disk from the HP.

16 Power on the monitor.

17 Power on the HP.

- The HP starts booting up.

18 At the **Selecting a system to boot. To stop selection process press and hold the ESCAPE key** message, press and hold **Escape**.

- You have 10 seconds to press **Escape** before the boot process proceeds.
- The boot process will stop and a menu of boot commands will appear.

19 Select boot scsi.6.0 by typing **b *DeviceSelectionForscsi.6.0***, press **Return**.

- For example, if the Device Selection for scsi.6.0 in the menu is P1 then type **b P1** and press **Return**.

20 At the **login:** prompt, type **root**, press **Return**.

21 Type ***RootPassword***, press **Return**.

- ***RootPassword*** is the root password for the download disk. (The HP uses the download disk's root password until a new one is set.)
- Remember that the ***RootPassword*** is case sensitive.
- You are authenticated as root and returned the UNIX prompt.

22 Type **passwd root**, press **Return**.

23 At the **New password:** prompt, type ***RootPassword***, press **Return**.

- ***RootPassword*** is the root password for the HP.
- Remember that the ***RootPassword*** is case sensitive.

24 At the **Re-enter new password:** prompt, type ***RootPassword***, press **Return**.

- ***RootPassword*** is the root password for the HP.
- This step confirms that the root password has been entered correctly.
- Remember that the ***RootPassword*** is case sensitive.
- The root password for this HP is set. Inform all authorized personnel of ***RootPassword***.

25 Type **exit**, press **Return**.

- Root is logged out of the HP.

26 Inform the backup administrator of the new machine.

To install the HP-UX 10.01 and 10.10 operating system, execute the steps provided in the following table.

Table 3.5-6 presents the **QUICK STEP** procedure required to install the HP-UX 10.01 and 10.10 operating system.

Table 3.5-6. Install the HP-UX 10.01 and 10.10 Operating System - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	**get the download disk**
2	(No entry)	**check that download disk is set to target 2**
3	(No entry)	**plug download disk into HP**
4	(No entry)	**power on download disk**
5	(No entry)	**power on monitor**
6	(No entry)	**power on HP**
7	(No entry)	**press and hold Escape**
8	b *DeviceSelectionForscsi.2.0* isl	**press Return**
9	hpux -is boot disk(scsi.2;0)/hp-ux	**press Return**
10	/download/setup	**press Return**
11	*HPsName*	**press Return**
12	*HPsIP*	**press Return**
14	/etc/shutdown -h -y now	**press Return**
15	(No entry)	**power off download disk**
16	(No entry)	**power off the monitor**
17	(No entry)	**power off the HP**
18	(No entry)	**disconnect download disk from HP**
19	(No entry)	**power on the monitor**
20	(No entry)	**power on the HP**
21	(No entry)	**press and hold Escape**
22	b *DeviceSelectionForscsi.6.0*	**press Return**
23	root	**press Return**
24	*RootPassword of download disk*	**press Return**
25	passwd root	**press Return**
26	*RootPassword for the HP*	**press Return**
27	*RootPassword for the HP*	**press Return**
28	exit	**press Return**
29	(No entry)	**inform all authorized personnel of *RootPassword for the HP***
30	(No entry)	**inform backup administrator of new HP**

3.5.2.2.3 IRIX 6.2 Operating Systems Installation

The IRIX 6.2 Operating Systems Installation process begins when procedure 3.5.2.1 Installation of Hardware has been completed in the Installing a New Workstation process. Once complete, the SA proceeds to procedure 3.5.2.3.1 Installation of Custom Software.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedure assumes that procedures 3.5.1 Preparation and 3.5.2.1 Installation of Hardware have been completed. The procedure also assumes that the workstation is powered off.

Table 3.5-7 presents the steps required to install the IRIX 6.2 operating systems in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

This section explains how to install the IRIX 6.2 operating systems, including network configuration and patch installation.

To install the IRIX 6.2 operating system, execute the procedure steps that follow:

1 Get the download disk.

2 Check that it is set to be target 2.

- The target number is found on the bottom of the disk.
- You can change the target number by hitting the buttons above and below it.

3 Plug the download disk into the SGI, if available; otherwise use CD-ROM skip to Step 5

4 Power on the download disk.

- The power switch is located on the back of the drive.

5 Power on the monitor; power on the SGI.

- The power switch is located on the front of the SGI, towards the left.

6 At the **Starting up the system**... message, click the **Stop for Maintenance** button.

- You have only a few seconds to click the **Stop for Maintenance** button before the boot process proceeds.
- The boot process will stop and a **System Maintenance** menu will appear.

7 Select **5 Enter Command Monitor**.

- You will be returned to the Command Monitor prompt which is >>.

8 At the >> prompt, type **hinv**, press **Return**.

- Verify that target 2 exists by finding it in the listing that appears. It will appear as **SCSI Disk: scsi(0)disk(2)**.

9 Type **boot -f dksc(0,2,0)sash**, press **Return**.

- The SGI boots from the download disk into the stand alone shell.
- You will be returned to a UNIX prompt.

10 Type **/download/setup**, press **Return**.

- Status messages will be displayed.

11 When prompted for the SGI's name, type ***SGIsName***, press **Return**.

12 When prompted for the SGI's IP address, type ***SGIsIP***, press **Return**.

- The SGI's network and hostname are configured.

13 When you are returned to a UNIX prompt, type **/etc/shutdown -y -g0**, press **Return**.

- The SGI shuts down.
- You will be returned to a >> prompt, a **System Maintenance** menu or a message saying that **this system can be powered off**.

14 Power off the download disk, power off the monitor.

15 Power off the SGI.

16 Disconnect the download disk from the SGI.

17 Power on the monitor.

18 Power on the SGI.

- The SGI starts booting up.

19 At the **login:** prompt, type **root**, press **Return**.

20 Type ***RootPassword***, press **Return**.

- ***RootPassword*** is the root password for the download disk. (The SGI uses the download disk's root password until a new one is set.)
- Remember that the ***RootPassword*** is case sensitive.
- You are authenticated as root and returned the UNIX prompt.

21 Type **passwd root**, press **Return**.

22 At the **New password:** prompt, type ***RootPassword***, press **Return**.

- ***RootPassword*** is the root password for the SGI.
- Remember that the ***RootPassword*** is case sensitive.

23 At the **Re-enter new password:** prompt, type ***RootPassword***, press **Return**.

- ***RootPassword*** is the root password for the SGI.
- This step confirms that the root password has been entered correctly.
- Remember that the ***RootPassword*** is case sensitive.
- The root password for this SGI is set. Inform all <u>authorized</u> personnel of ***RootPassword***.

24 Type **exit**, press **Return**.

- Root is logged out of the SGI.

25 Inform the backup administrator of the new machine.

To install the IRIX 6.2 operating system, execute the steps provided in the following table.

Table 3.5-7. Install the IRIX 6.2 Operating System - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	**get the download disk**
2	(No entry)	**check that download disk is set to target 2**
3	(No entry)	**plug download disk into SGI**
4	(No entry)	**power on download disk**
5	(No entry)	**power on monitor**
6	(No entry)	**power on SGI**
7	(No entry)	**click the Stop for Maintenance button**
8	5 Enter Command Monitor	**(No action)**
9	hinv	**press Return**
10	(No entry)	**verify that SCSI Disk: scsi(0)disk(2) appears in the listing**
11	boot -f dksc(0,2,0)sash	**press Return**
12	/download/setup	**press Return**
13	*SGIsName*	**press Return**
14	*SGIsIP*	**press Return**
15	/etc/shutdown -y -g0	**press Return**
16	(No entry)	**power off download disk**
17	(No entry)	**power off monitor**
18	(No entry)	**power off SGI**
19	(No entry)	**disconnect download disk from SGI**
20	(No entry)	**power on monitor**
21	(No entry)	**power on SGI**
22	root	**press Return**
23	*RootPassword of download disk*	**press Return**
24	passwd root	**press Return**
25	*RootPassword for the SGI*	**press Return**
26	*RootPassword for the SGI*	**press Return**
27	exit	**press Return**
28	(No entry)	**inform all authorized personnel of *RootPassword for the SGI***
29	(No entry)	**inform backup administrator of new SGI**

3.5.2.2.4 NCD Operating System Installation

The NCD Operating System Installation process begins when procedure 3.5.2.1 Installation of Hardware has been completed in the Installing a New Workstation process. Once complete, the SA proceeds to procedure 3.5.3 Testing and Verification.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedure assumes that procedures 3.5.1 Preparation and 3.5.2.1 Installation of Hardware have been completed. The procedure also assumes that the workstation is powered off.

Installing the NCD operating system consists of configuring the NCD.

Table 3.5-8 presents the steps required to configure the NCD in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

This section explains how to configure the NCD, including putting the necessary start-up files in place on the server.

To configure the NCD, execute the procedure steps that follow:

1 Turn on the NCD and monitor. The monitor power button is on the lower front of the monitor. The NCD power switch is on the back, on the right.

- The message **Boot Monitor V*x.x.x*** will appear.

2 Press the **Escape** key twice.

- You have only a few seconds to press the **Escape** key.
- The boot process stops and a boot monitor prompt, >, appears.
- If you do not see a > prompt then press the **Escape** key a few more times.

3 Press the **Setup** key.

- The **Main** menu will appear.

4 Go to the **Keyboard** menu by pressing the **Right Arrow** key.

- The **Keyboard** menu appears.

5 Select **N-101** by pressing the **Down Arrow** key.

- You may need to press the **Down Arrow** key a few times before **N-101** is selected.

6 Go to the **Monitor** menu by pressing the **Right Arrow** key.

- The **Keyboard** menu disappears.
- The **Monitor Resolution** menu appears.

7 Select **1600x1200 65 Hz** by pressing the **Down Arrow** key.

- You may need to press the **Down Arrow** key a few times before **1600x1200 65 Hz** is selected.

8 Press the **Shift** and **T** keys.

- This tests the new monitor resolution setting.

9 Use the **+** and **-** keys on the front of the monitor under the **ADJUST** label to adjust the screen.

10 Press the **STORE** key on the front of the monitor.

- The monitor stores the screen adjustments.

11 Press the **Escape** key.

- The monitor resolution test ends.
- You are returned to the **Main** menu.

12 Go to the **Network** menu by pressing the **Right Arrow** key twice.

- The **Monitor Resolution** menu disappears.
- The **Network** menu appears.

13 Select **NVRAM** for the **Get IP Addresses From** option.

- You can use the **Space Bar** to move between the available options.

14 Press the **Down Arrow** key.

15 Type the ***NCDIPaddress*** for the **Terminal IP Address** option, press the **Down Arrow** key.

- The ***NCDIPaddress*** is in dotted decimal notation, for example, 155.157.21.34.

16 Type the ***StartupFileServerIPaddress*** for the **First Boot Host IP Address** option, press the **Down Arrow** key.

- The ***StartupFileServerIPaddress*** is in dotted decimal notation, for example, 155.157.44.22.
- The ***StartupFileServer*** is the machine where the NCD startup files are stored.

17 Press the **Down Arrow** key twice.

18 Type the ***NCDGatewayIPaddress*** for the **Gateway IP address** option, press the **Down Arrow** key.

- The ***NCDGatewayIPaddress*** is in dotted decimal notation, for example, 155.157.44.22.
- The ***NCDGatewayIPaddress*** is the same as the ***NCDIPaddress*** except the last number/octet is 1. For example, if the ***NCDIPaddress*** is 155.157.21.34, the ***NCDGatewayIPaddress*** is 155.157.21.1.

19 Press the **Down Arrow** key, type the ***BroadcastIPaddress*** for the **Broadcast IP Address** option.

- The ***BroadcastIPaddress*** is in dotted decimal notation, for example, 155.157.44.22.
- The ***BroadcastIPaddress*** is the same as the ***NCDIPaddress*** except the last number/octet is 255. For example, if the ***NCDIPaddress*** is 155.157.21.34, the ***BroadcastIPaddress*** is 155.157.21.255.

20 Press the **Right Arrow** key.

- The **Network** menu disappears.
- The **Boot** menu appears.

21 Type **Xncdhmx_s** for the **Boot File** option, press the **Down Arrow** key.

22 Press the **Down Arrow** key, type **/data/ncd/** for the **NFS Boot Directory** option, press the **Down Arrow** key.

23 Press the **Down Arrow** key, type **/usr/lib/X11/ncd/configs/** for the **UNIX Config Directory** option, press the **Down Arrow** key.

24 Press the **Down Arrow** key, press the **d** key.

- The **TFTP Order** option is set to **Disabled**.

25 Press the **Down Arrow** key, press the **1** key.

- The **NFS Order** option is set to **1**.

26 Press the **Down Arrow** key, press the **d** key.

- The **MOP Order** option is set to **Disabled**.

27 Press the **Down Arrow** key, press the **d** key.

- The **LOCAL Order** option is set to **Disabled**.

28 Press the **Right Arrow** key.

- The **Boot** menu disappears.
- The **Done** menu appears.
- **Reboot** is selected.

29 Press the **Return** key.

- The NCD reboots.
- Status messages appear.

30 Log into the ***StartupFileServer*** by typing: **telnet *StartupFileServer*** or **rsh *StartupFileServer*** at a UNIX prompt, then press **Return**.

31 If a **Login:** prompt appears, log in as yourself by typing: ***YourUserID***, then press **Return**.

- A password prompt is displayed.

32 Enter ***YourPassword***, then press **Return.**

- Remember that ***YourPassword*** is case sensitive.
- You are authenticated as yourself and returned to the UNIX prompt.

33 Log in as root by typing: **su**, then press **Return**.

- A password prompt is displayed.

34 Enter the ***RootPassword*,** then press **Return**.

- Remember that the ***RootPassword*** is case sensitive.
- You are authenticated as root and returned to the UNIX prompt.

35 Type **cd /usr/lib/X11/ncd/configs**, press **Return**.

36 Type **./i**, press **Return**.

- **i** is a script which builds a NCD startup file.

37 Type the last two numbers/octets of the ***NCDIPaddress*** when the script prompts you for the **IP address**, press **Return**.

- For example, if the ***NCDIPaddress*** is 155.157.21.34 then type **21.34** and then press **Return**.

38 Type the ***NCDLoginHost*** when the script prompts you for the **Login Host**, press **Return**.

- The ***NCDLoginHost*** is the name of one of the X-servers.

39 When the script prompts you for the **NCD Number**, type the ***NCDname*** minus the ncd part.

- For example, if the ***NCDname*** is ncd2 then the **NCD Number** is 2.
- Some status messages appear telling you what the script is doing.
- The script exits.

40 Type **exit**, then press **Return**.

- **Root** is logged out

41 Type **exit** again, then press **Return**.

- You are logged out and disconnected from the ***StartupFileServer.***

To configure the NCD, execute the steps provided in the following table.

Table 3.5-8. Configure the NCD - Quick-Step Procedures (1 of 2)

Step	What to Enter or Select	Action to Take
1	(No entry)	**power on the monitor and NCD**
2	(No entry)	**press Escape twice**
3	(No entry)	**press Setup key**
4	(No entry)	**press Right Arrow key**
5	N-101	**press Right Arrow key**
6	1600x1200 65 Hz	**press Shift and T keys**
7	(No entry)	**use + and - keys under ADJUST on front of monitor to adjust the screen**
8	(No entry)	**press the STORE key on the front of the monitor**
9	(No entry)	**press Escape**
10	(No entry)	**press Right Arrow key twice**
11	NVRAM	**press Down Arrow key**

Table 3.5-8. Configure the NCD - Quick-Step Procedures (2 of 2)

12	*NCDIPaddress*	**press Down Arrow key**
13	*StartupFileServerIPaddress*	**press Down Arrow key three times**
14	*NCDGatewayIPaddress*	**press Down Arrow key twice**
15	*BroadcastIPaddress*	**press Right Arrow key**
16	Xncdhmx_s	**press Down Arrow key twice**
17	/data/ncd/	**press Down Arrow key twice**
18	/usr/lib/X11/ncd/configs/	**press Down Arrow key twice**
19	(No entry)	**press d key**
20	(No entry)	**press Down Arrow key**
21	(No entry)	**press 1 key**
22	(No entry)	**press Down Arrow key**
23	(No entry)	**press d key**
24	(No entry)	**press Down Arrow key**
25	(No entry)	**press d key**
26	(No entry)	**press Right Arrow key**
27	(No entry)	**press Return**
28	telnet *StartupFileServer* -or- rsh *StartupFileServer*	**press Return**
29	*YourUserID*	**press Return**
30	*YourPassword*	**press Return**
31	su	**press Return**
32	*RootPassword*	**press Return**
33	cd /usr/lib/X11/ncd/configs	**press Return**
34	./i	**press Return**
35	last two numbers/octets of *NCDIPaddress*	**press Return**
36	*NCDLoginHost*	**press Return**
37	*NCDname* minus the ncd part	**press Return**
38	exit	**press Return**
39	exit	**press Return**

3.5.2.3 Software

3.5.2.3.1 Custom

The Installation of Custom Software process begins when procedure 3.5.2.2 Operating System Installation has been completed in the Installing a New Workstation process. Once complete, the SA proceeds to procedure 3.5.2.3.2 Installation of COTS Software.

Detailed procedures for tasks performed by the SA are provided below. The procedure assumes that procedures 3.5.1 Preparation, 3.5.2.1 Installation of Hardware and 3.5.2.2 Operating System Installation have been completed.

Table 3.5-9 presents the steps required to install custom software in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

To install custom software for the requester, execute the procedure step that follows:

1 execute procedures in Section 22.2.3 Custom Software Installation in this document.

To install custom software, execute the steps provided in the following table.

Table 3.5-9. Install Custom Software - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	**execute procedures in Section 22.2.3 of this document**

3.5.2.3.2COTS

The COTS Software Installation process begins after the SA has completed Section 3.5.2.3.1 Custom Software Installation. After the COTS software installation is complete, the SA proceeds to procedure 3.5.3 Testing and Verification.

Detailed procedures for tasks performed by the SA are provided below. The procedure assumes that procedures 3.5.1 Preparation, 3.5.2.1 Installation of Hardware, 3.5.2.2 Operating System Installation and 3.5.2.3.1 Custom Software Installation have been completed.

Table 3.5-10 contains a table which presents the steps required to install COTS software in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

To install COTS software for the requester, execute the procedure steps that follow:

1 Refer to the Release A Hardware and Software Mapping Baseline (attached at the end of this document) for your site.

- For LaRC, refer to document number 420-TD-007-001.
- For SMC, refer to document number 420-TD-008-001.
- For GSFC, refer to document number 420-TD-006-001.

2 In the Release A Hardware and Software Mapping Baseline for your site, look up which COTS packages need to be installed on the new workstation using the **Subsystem** and hardware type (the **Target Operating System** column in the document) of the new machine.

To install COTS software, execute the steps provided in the following table.

Table 3.5-10. Install COTS Software - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	**refer to the Release A Hardware and Software Mapping Baseline for your site**
2	(No entry)	**look up which COTS packages to install using the Subsystem and Target Operating System of the new workstation**

3.5.3 Testing and Verification

3.5.3.1 Reboot

The Reboot process begins when procedure 3.5.2.3.2 COTS - By Package has been completed in the Installing a New Workstation process. Once complete, the SA proceeds to procedure 3.5.3.2 Logging In.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that procedures 3.5.1 Preparation and 3.5.2 Installation have been completed.

Table 3.5-11 presents the steps required to reboot in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

3.5.3.1.1SGI, HP and Sun

To reboot, execute the procedure steps that follow:

1 At the UNIX prompt for the workstation, type **su**, press **Return**.

2 At the **Password** prompt, type ***RootPassword***, press **Return**.

- Remember that ***RootPassword*** is case sensitive.
- You are authenticated as root.

3 Type **who**, press **Return**.

- A list of users currently logged into the workstation appears.

4 If users other than root and you are logged in:
type **wall**,
press **Return**,
type **The system is going down in 5 minutes for *Reason*. Please save your work and log off. We apologize for the inconvenience.**,
press **Return**,
press **Control-D**,

wait 5 minutes before proceeding to step 5.

5 Type **/etc/reboot**, then press **Return**.

- The workstation reboots.
- Watch the status messages that appear for any errors.
- If you are returned to a **Login** prompt and saw no errors during the reboot, the reboot was successful.
- If the reboot was unsuccessful, use the error messages and system logs to figure out what is incorrect in the workstation installation. The system logs are: /var/adm/messages for Solaris 2.5.1/5.4, /var/adm/SYSLOG for IRIX 5.3 and 6.2, and /usr/adm/syslog and rc.log for HP-UX 10.01 and 10.10.

To reboot, execute the steps provided in the following table.

Table 3.5-11. Reboot - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	su	**press Return**
2	*RootPassword*	**press Return**
3	who	**press Return**
4	wall	**press Return**
5	The system is going down in 5 minutes for *Reason*. Please save your work and log off. We apologize for the inconvenience.	**press Return**
6	(No entry)	**press Control-D**
7	(No entry)	**wait 5 minutes**
8	/etc/reboot	**press Return**
9	(No entry)	**watch for errors in the boot messages**

3.5.3.1.2 NCD

The Reboot the NCD process begins when procedure 3.5.2.3.2 COTS - By Package has been completed in the Installing a New Workstation process. Once complete, the SA proceeds to procedure 3.5.3.2 Logging In.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that procedures 3.5.1 Preparation and 3.5.2 Installation have been completed.

To reboot the NCD, execute the procedure steps that follow:

1 Press the **Setup** key.

- The **NCD User Services: Console** window will appear.

2 Go to the **Console** menu, select **Reboot**.

- The **Reboot** window opens asking if it is **OK to reboot the terminal**.

3 Click the **OK** button.

- The NCD reboots.
- Watch the status messages that appear.
- Once the NCD successfully reboots, a login screen appears.
- If the NCD does not successfully reboot then use the information in the status messages to determine what went wrong in procedure 3.5.2.2.4 NCD Operating System Installation.

Table 3.5-12 presents the **QUICK STEP** procedure required to reboot the NCD.

Table 3.5-12. Reboot the NCD - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	**press Setup key**
2	Console → Reboot	**click OK button**
3	(No entry)	**watch for errors in the boot messages**

3.5.3.2 Logging In

The Logging In process begins when procedure 3.5.3.1 Reboot has been completed in the Installing a New Workstation process. Once complete, the SA proceeds to procedure 3.5.3.3 Test Environment.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that procedures 3.5.1 Preparation, 3.5.2 Installation and 3.5.3.1 Reboot have been completed. The procedures also assume that the workstation is currently at a **Login** prompt.

Table 3.5-13 presents the steps required to log in in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

To log in, execute the procedure steps that follow:

1 At the **Login** prompt for the workstation, type ***YourUserID***, press **Return**.

2 At the **Password** prompt, type ***YourPassword***, press **Return**.

- Remember that ***YourPassword*** is case sensitive.
- You are logged in and authenticated as yourself.
- You are returned to a UNIX prompt.

- If you are not logged in and returned to a UNIX prompt, logging in was unsuccessful. Follow these steps:

  a Execute this procedure one more time.
  If logging in is unsuccessful again, there is a problem with the workstation installation. Continue to step b.

  b Type **root** at the **Login** prompt, press **Return**.

  c Type ***RootPassword*** at the **Password** prompt, press **Return**.
  Remember that ***RootPassword*** is case sensitive.
  You are authenticated as root and returned to a UNIX prompt.

  d Check that automount is running by typing **ps -ef | grep auto** or **ps -aux | grep auto**, press **Return**.
  If automount is running then you will see output similar to this:

```
yourID   10173  0.2  0.4  648  408 pts/38   S 15:35:51  0:00 grep auto
root       140      0.0  0.8  1796 1004 ?       S  Jun 25    2:40 /usr/lib/autofs/
                                                              automountd -D ARCH=sun5
```

  If automount is not running then run it by typing:
  /usr/lib/autofs/automountd -D ARCH=sun5 for Solaris 2.5.1/5.4,
  /usr/etc/automount -D ARCH=sgi for IRIX 5.3 and 6.2,
  /usr/etc/automount -D ARCH=hp for HP-UX 10.01 and 10.10,
  press **Return**.
  Try logging in again by typing **su -** ***YourUserID***, press **Return**, type***YourPassword***, press **Return**. Type **whoami** and press **Return** to confirm that you successfully logged in as yourself and type **cd**, press **Return**, type **pwd**, press **Return** to confirm that you are in your home directory. If these commands return ***YourUserID*** and your home directory, you have successfully logged in. If you have not successfully logged in, proceed to step e.

  e The workstation probably did not successfully bind to a NIS server. Verify that
  the NIS server is up and on the network. Once it is, execute procedure 3.5.3.1
  Reboot and then execute this procedure again.

To log in, execute the steps provided in the following table.

Table 3.5-13. Log In - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	*YourUserID*	**press Return**
2	*YourPassword*	**press Return**

3.5.3.3 Test Environment

The Test Environment process begins when procedure 3.5.3.2 Logging In has been completed in the Installing a New Workstation process. Once the test environment procedure is complete, the Installing a New Workstation process is complete and the SA notifies the requester, the supervisor and the DAAC Manager.

Table 3.5-14. Test Environment - Activity Checklist

Order	Role	Task	Section	Complete ?
1	SA	Test Environment.	(P) 3.5.3.3.1	
2	SA	Inform Requester, Supervisor and DAAC Manager of completion.	(I) 3.5.3.3.1	

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that procedures 3.5.1 Preparation, 3.5.2 Installation, 3.5.3.1 Reboot and 3.5.3.2 Logging In have been completed.

Table 3.5-15 presents the steps required to test the environment in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

To test the environment, execute the procedure steps that follow:

1 At the UNIX prompt, type **ps -ef | more** or **ps -aux | more**.

- A screen full of information about the currently running processes is displayed.

2 Look for the processes associated with the custom and COTS software which you installed in the process listing.

- To move to the next page full of information, press the **Space** bar.
- If a process is missing in the listing, go back to the installation of that software package to determine what went wrong.

3 Type **cd** ~/***YourUserID***, press **Return**.

4 Type **pwd**, press **Return**, use the output to verify that you are in your home directory.

- This verifies that automount is running and working correctly for the NIS map auto.home. You may follow steps similar to steps 3 and 4 for the other NIS maps.
- This also verifies that the new workstation was able to contact a NIS server.

To test the environment, execute the steps provided in the following table.

Table 3.5-15. Test Environment - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	**ps -ef -or- ps -aux**	**press Return**
2	(No entry)	**find processes associated with the installed custom and COTS software packages in the listing**
3	(No entry)	**press Space bar for the next page of process information**
4	**cd *~/YourUserID***	**press Return**
5	**pwd**	**press Return**
6	(No entry)	**use the output to verify that you are in your home directory**

3.6 DCE Configuration

3.6.1 Configuring Initial Cell

The Configuring the Initial Cell consists of configuring the Master Security Server, initial CDS Server and DTS Servers (Time & Time Provider servers). This section describes how to configure the Master Security server and initial CDS server. Section 3.6.2 explains setting up the DTS server(s).

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that all planning involved has been concluded well in advance and the SA has been properly trained to perform the configuration.

Table 3.6-1 presents the steps required to configure the initial cell in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

This section explains how to configure the initial cell. To begin configuring the initial cell, execute the procedures steps that follow:

NOTE: When planning a DCE cell, note that you must configure a CDS client on any Security server system that is not running a CDS server. You must also configure a Time client on any system that is not running a Time server. Be sure to configure these clients only after you have configured all servers.

1 Log in as root on the system you wish to configure

2 Make sure that /etc is in your command search path:

```
#export PATH=/etc:$PATH (Bourne/Korn shell)

% setenv PATH /etc:$PATH (C shell)
```

3 Type in the following appropriate command:

The sun command is dcesetup config client

The IBM command is mkdce -a cell_admin

-s edf-bb.gsfc.nasa.gov -c edf-bb.gsfc.nasa.gov cds_cl

The HP OSF DCE command is dce_config

Example:

```
<baltic /home/reginald>dce_config  (HP OSF DCE command)
```

4 From the DCE Main Menu, select configure and start DCE deamons (selection 1).

5 From the DCE Configuration Menu, select Initial Cell Configuration (selection 1).

6 From the Initial Cell Configuration Menu, select Security Server (selection 1).

7 If this is your very first cell configuration, or if you have previously run REMOVE, answer **n** to the following question. If you are re-configuring a cell, answer **y**.

> Do you wish to first remove all remnants of previous DCE configurations for all components (y/n)?
>
> You should do so only if you plan on re-configuring all existing DCE components now: (n)

8 Enter the name of your cell (without /.../).
dce_config will prompt you with a warning. If rpcd was recently running with the TCP protocol sequence, then wait until 4 minutes have elapsed since rpcd was stopped before continuing from this prompt:

9 Enter keyseed for initial database master key:

1 0 dce_config prompts you to choose the Cell Administrators' principal name and password. The default principle name for the Cell Administrator is cell_admin:

11 dce_config prompts you for the starting point for UNIX user and group ID's that will be generated by the DCE Security Service. This step prevents the DCE Security Service from generating IDs that are already in use by your system. Type <RETURN> to choose the default value, or enter a value of our choice:

1 2 Enter the starting point to be used for UNIX ID'S that are automatically generated by the Security Service when a principal is added using "rgy_edit": (N +100) <RETURN>

This system is now configured as the Master Security server. You must now create a CDS server, either on this system or on another system.

If the CDS server for this cell will be on another system, repeat the steps 1-4 above on that system, then continue with Step 13.

If the CDS server is on the same system as the Security server, continue with Step 14 below.

1 3 From the DCE Configuration Menu, select Initial Cell Configuration (selection 1)

14 From the Initial Cell Configuration menu, choose Initial CDS Server (selection 2) This routine starts up cdsadv and cdsd, initializes the namespace, and sets ACLs for all new namespace entries.

15 dce_config asks if your cell resides on multiple LAN's. If your cell does reside on multiple LAN's, dce_config asks for the name of the LAN. The name you provide is arbitrary, and is used by dce_config to store cell profile information.

Table 3.6-1. Configuring Initial Cell - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	**Login as root**
2	(No entry)	**Make sure that /etc is in your command search path**
3	(No entry)	**type appropriate setup command**
4	(No entry)	**select 1 from DCE Main Menu**
5	(No entry)	**select 1 from the DCE Configuration Menu**
6	(No entry)	**select 1 from the Cell Configuration Menu**
7	(No entry)	**If reconfiguring, answer yes.** **If not reconfiguring, answer no.**
8	(No entry)	**Enter cell name**
9	(No entry)	**Enter keyseed.**
10	(No entry)	**Enter principal name and password.**
11	(No entry)	**Press <return> for default or enter a value.**
12	(No entry)	**Press <return> or enter value**
13	(No entry)	**select 1 from DCE Configuration Menu**
14	(No entry)	**select 2 from Initial Cell Configuration Menu**
15	(No entry)	**Enter arbitrary LAN name.**

3.6.2 Configuring DTS Servers

The Configuring the DTS Servers process begins after the Master CDS server has been configured. Refer to section 3.6.1 Configuring Initial Cell for Master CDS Server Configuration procedures before continuing with this section.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that all planning involved has been concluded well in advance and the SA has been properly trained to perform the configuration.

Table 3.6-2 presents the steps required to configure DTS servers in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

This section explains how to configure the DTS daemon. To begin configuring the DTS daemon, execute the procedures steps that follow:

NOTE: To configure a DTS server on a system not already configured as a Security or Directory server, repeat steps 1-4 of Section 3.6.1.1 (Configuring the Initial Cell) on that system, and then continue with the steps below. To configure a DTS server on a system already configured as a Security or Directory server, continue with step 1 below.

1 From the DCE Configuration menu, select Additional Server Configuration (selection 2).

2 From the Additional Server Configuration menu, select DTS (selection 2).

3 From the DTS Configuration menu, select DTS Local Server for servers on the LAN (selection 1). Otherwise, select DTS global server (selection 2). Either selection starts the dts daemon (dtsd) and dtstimed.

4 Configure a DTS time provider on one of the time servers in a cell. Select the DTS Time Provider (selection 4).

The DTS null time provider configures a system to trust its own clock as an accurate source of time. The DTS ntp provider obtains an accurate source of time from some other system outside the cell. See the OSF DCE Administration Guide for more information on time providers.

5 From the DTS Time Provider Menu, select Null Time Provider (selection 1) or NTP Time Provider (selection 2).

If you select the NTP time provider the following prompt appears: Enter the host name where the NTP server is running:

6 Enter the host name.

Table 3.6-2. Configuring DTS Servers - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	**select 2 from DCE Configuration Menu**
2	(No entry)	**select 2 from Additional Server Configuration Menu**
3	(No entry)	**select 1 for servers on the same LAN or select 2 from the DTS Configuration Menu**
4	(No entry)	**select 4 to configure DTS time provider**
5	(No entry)	**select 1 or 2 from DTS Time Provider Menu**
6	(No entry)	**enter the host name where the NTP server is running**

3.6.3 Configuring Additional CDS Servers

The Configuring Additional CDS Servers process begins after the DTS servers have been configured. Refer to section 3.6.2 procedures before continuing with this section.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that all planning involved has been concluded well in advance and the SA has been properly trained to perform the configuration.

Table 3.6-3 presents the steps required to configure additional CDS servers in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

This section explains how to configure additional CDS servers. To begin configuring the additional CDS servers, execute the procedures steps that follow:

1 From the DCE Configuration menu, select Additional Server Configuration (selection 2).

2 Enter the name of your cell.

3 Enter the host name of your cell's security server**.**

Make sure the contents of the pe_site file is identical on both the server and the client. The dce_config script checks this, but prompts for your confirmation. Identical pe_site files are normally generated automatically, but you should confirm this yourself, particularly during your initial set-up. If the pe_site files are not identical, you should start this procedure again.

Ensure the /opt/dcelocal/etc/security/pe_site file matches that on the server...

4 Press <RETURN> to continue, CTRL-C to exit: <RETURN>

5 Enter the cell administrator's principal name and password.

6 From the Additional Server Configuration menu, select Additional CDS Server(s) (selection 1).

7 Enter the name of the cell CDS server. If the cell has more than one CDS server, choose one.

8 dce_config asks if more directories should be replicated. If you answer **yes**, continue to step 9.

9 Enter a list of directories to be replicated, separated by spaces and terminated by <RETURN>.

Notes on Configuring Additional CDS Servers

Immediately after configuring an additional CDS server, you should skulk the root directory using the set directory /.: to skulk command as cell_admin in cdscp. This will initiate the propagation of a consistent copy of the changed root directory information to all the CDS servers, and will prevent problems which might arise from use of inconsistent information before this propagation. The use of several CDS servers may increase the time required to complete the propagation of this information.

Configuration of additional CDS servers can occasionally fail if namespace information is not correctly propagated. Typical failures observe from this cause are:

```
ERROR:    Error during creation of clearinghouse /.:/nodename_ch.

          Message from cdscp:

          Failure in routine:  cp_create_clh; code = 282109010

          Requested operation would result in lost connectivity to root directory (dce /
          cds)

ERROR:    Error during creation of clearinghouse / .:/nodename_ch.

Message from cdscp:

          Failure in routine:  cp_create_clh; code = 282108908

          Unable to communicate with any CDS server (dce / cds)
```

If this happens, the server daemon cdsd has been successfully launched, but its clearinghouse has not bee properly created. the clearinghouse is in an intermediate state and cannot be used or deleted, although the rest of the cell namespace an other servers are unaffected. To recover, skulk the root directory, and then use the create clearinghouse /.:/nodename_ch command as cell_admin in cdscp on the new CDS server node to manually complete the configuration of the new server and its clearinghouse. Then skulk the root directory again.

In rare circumstances, you may see the following error when configuring a CDS client or additional server:

```
ERROR:    cdscp error during "define cached server" command.

          Message from cdscp:

          Failure in routine:  cp_define_cached_server; code = 282111142

          Cached Server clearinghouse already exists (dce / cds)
```

This error is benign and results from the system trying to repeat an operation that has already been done. This error may be ignored.

Table 3.6-3. Configuring Additional CDS Servers - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	select 2 from the DCE Configuration menu
2	(No entry)	Enter the name of your cell
3	(No entry)	Enter the host name of your cell's security server
4	(No entry)	press <return> to continue or CTRL-C to exit
5	(No entry)	Enter the cell administrator's principal and password
6	(No entry)	select 1 from the Additional Server Configuration menu
7	(No entry)	Enter the name of the cell CDS server

8	(No entry)	answer yes and continue to step 9 or answer no to end process
9	(No entry)	Enter a list of directories to be replicated

3.6.4 Configuring Security and CDS Client Systems

Before configuring clients, configure server systems as described in the Initial Cell Configuration, Configuring DTS Servers, and Configuring Additional CDS Servers sections. Then use this procedure to configure client systems.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that all planning involved has been concluded well in advance and the SA has been properly trained to perform the configuration.

Table 3.6-4 presents the steps required to configure security and CDS client systems in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

This section explains how to configure security and CDS client systems. To begin configuring the security and CDS client systems, execute the procedures steps that follow:

You must configure a CDS client on any Security server system that is not running a CDS server. To configure a client system, you need to know the name of the Security server and the initial CDS server for the cell.
Note that this procedure does not create a DTS clerk (client). This is described in section 3.6.5.

1 Start dce_config on the system that you wish to configure with DCE client(s).

2 From the DCE Main menu, select Configure (selection 1).

3 From the DCE Configuration menu, select DCE Client (selection 3).

4 Enter the name of your cell.

5 Enter the name of the security server for the cell. Then press <RETURN> to continue, CTRL-C to exit: <RETURN>

6 Enter the cell administrator's principal name and password.

7 Enter the name of a CDS server in this cell. If there is more than one, first enter the name of the server to be cached, if necessary. Then continue with the next server(s).

You will be asked whether or not this node is to be configured as a DFS client. Answer **no**.

8 You will now be asked to create a LAN profile so clients and servers can be divided into profile groups for higher performance in a multi-lan cell. Answer **no**.

9 You will now be asked if this machine should be configured as a DTS Clerk, DTS Local Server or DTS Global Server (the default is DTS Clerk). Type **local**.

Table 3.6-4. Configuring Security and CDS Client Systems - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	**start dce_config**
2	(No entry)	**select 1 from DCE Main menu**
3	(No entry)	**select 3 from DCE Configuration menu**
4	(No entry)	**Enter the name of your cell**
5	(No entry)	**Enter the name of the security server for the cell**
6	(No entry)	**Enter the cell administrator's principal name and password**
7	(No entry)	**Enter the name of a CDS server in this cell**
8	(No entry)	**answer no for the node to be configured as a DFS client**
9	(No entry)	**type local for DTS Local Server**

3.6.5 Configuring DTS Clerks

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that all planning involved has been concluded well in advance and the SA has been properly trained to perform the configuration.

Table 3.6-5 presents the steps required to configure DTS clerks in a condensed manner. If you are already familiar with the procedures, you may prefer to use the quick-step tables. If you are new to the system, or have not performed this task recently, you should use the detailed procedures presented below.

This section explains how to configure DTS clerks. To begin configuring the DTS clerks, execute the procedures steps that follow:

You must configure a DTS clerk (client) on any system not running a DTS server. A DTS clerk is not stared automatically via the dce_config DCE Client menu option; you must explicitly start a DTS clerk from the DTS menu under Additional Server Configuration.

1 Start dce_config on the system that you wish to configure with a DTS clerk.

2 From the DCE Main menu, select Configure (selection 1).

3 From the DCE Configuration menu, select Additional Server Configuration (selection 2).

4 From the Additional Server Configuration menu, select DTS (selection 2).

5 From the DTS Configuration menu, select DTS Clerk (selection 3).

This node is now a DTS clerk.

Table 3.6-5. Configuring DTS Clerks - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	**start dce_config**
2	(No entry)	**select 1 from DCE Main menu**
3	(No entry)	**select 2 from DCE Configuration menu**
4	(No entry)	**select 2 from Additional Server Configuration menu**
5	(No entry)	**select 3 from DTS Configuration menu**

3.6.6 Configuring GDA Servers

The DCE Global Directory Agent (GDA) facilitates communication between DCE cells. This section describes how to start the GDA server. A GDA server can only be configured on an exiting client system or CDS server system.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that all planning involved has been concluded well in advance and the SA has been properly trained to perform the configuration.

Table 3.6-6 presents the steps required to configure GDA servers in a condensed manner. If you are already familiar with the procedures, you may prefer to use the quick-step tables. If you are new to the system, or have not performed this task recently, you should use the detailed procedures presented below.

This section explains how to configure GDA servers. To begin configuring the GDA servers, execute the procedures steps that follow:

1 From the DCE Main menu, select Configure (selection 1).

2 From the DCE Configuration menu, select Additional Server Configuration (selection 2).

3 From the Additional Server Configuration menu, select GDA Server (selection 7).

The system configures the GDA server and starts the GDA server daemon, gdad.

Table 3.6-6. Configuring GDA Servers - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	**select 1 from DCE Main menu**
2	(No entry)	**select 2 from DCE Configuration menu**

3	(No entry)	**select 7 from Additional Server Configuration menu**

3.6.7 Creating Security Server Replica

A new feature of HP DCE/9000 is Security Server Replication, which provides for improved cell performance and reliability. These steps will allow you to create a security replica via dce_config.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that all planning involved has been concluded well in advance and the SA has been properly trained to perform the configuration.

Table 3.6-7 presents the steps required to create a security server replica in a condensed manner. If you are already familiar with the procedures, you may prefer to use the quick-step tables. If you are new to the system, or have not performed this task recently, you should use the detailed procedures presented below.

This section explains how to create a security server replica. To begin creating a security server replica, execute the procedures steps that follow:

1 From the DCE Main menu, select Configure (selection 1).

2 From the DCE Configuration menu, select Additional Server Configuration (selection 2).

3 From the Additional Server Configuration menu, select Replica Security Server (selection 8).

4 Enter the keyseed for the initial datatbase master key.

The default name for the replica is subsys/dce/sec/$HOSTNAME. If you wish to change the name of the security replica that is created by dce_config, change the value of SEC_REPLICA, either in the file /opt/dcelocal/etcdce_com_env or in the shell environment from which dce_config is run. Note that you must do this before running dce_config.

Table 3.6-7. Creating a Security Server Replica - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	**select 1 from DCE Main menu**
2	(No entry)	**select 2 from DCE Configuration menu**
3	(No entry)	**select 8 from Additional Server Configuration menu**
4	(No entry)	**Enter keyseed for initial database master key**

3.6.8 Unconfiguring DCE Client

The UNCONFIGURE option removes the target machine from the cell Security database and the CDS namespace. DCE daemons must be running on the system executing the UNCONFIGURE option If daemons have been stopped, use the START option on the DCE Main Menu to restart them before using UNCONFIGURE. A successfully configured client system can be unconfigured locally. If there were any errors in configuring the client system as a security or directory service client, then the client must be unconfigured from some other system in the cell. Do not use the UNCONFIGURE option on a system that is used as a Security server or a CDS server. The UNCONFIGURE option removes the system from a cell. If the system is used as a Security server or a CDS server, UNCONFIGURE will break the cell.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that all planning involved has been concluded well in advance and the SA has been properly trained to perform the configuration.

Table 3.6-8 present the steps required to unconfigure a DCE client in a condensed manner. If you are already familiar with the procedures, you may prefer to use the quick-step tables. If you are new to the system, or have not performed this task recently, you should use the detailed procedures presented below.

This section explains how to Unconfigure a DCE Client. To begin Unconfiguring DCE Client, execute the procedures steps that follow:

1 From the DCE Main menu, select Unconfigure (selection 4).

2 Enter the host name of the node to be unconfigured.

3 Unconfiguring a node will remove the node's ability to operate in the cell. A reconfiguration of the node will be required.

4 You will be asked if you wish to continue. Type **y** to continue.

5 Enter the Cell Administrator's principal name and password.

WARNING: A dce_config REMOVE will need to be performed from node baltic before reconfiguring it.

6 From the DCE Main menu, select Remove (selection).

Remove will remove the node's ability to operate in the cell. A reconfiguration of the node will be required. If this is not a server node, then this node should be unconfigured before a REMOVE is done.

7 You will again be asked if you wish to continue. Type **y** to continue.

8 From the DCE Configuration menu, select Exit (selection 99).

You have now exited from dce_config.

Table 3.6-8. Unconfiguring DCE Client - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	**select 4 from DCE Main menu**
2	(No entry)	**enter host name of node to be configured**
3	(No entry)	**type y to continue**
4	(No entry)	**enter Cell Administrator's principal name and password**
5	(No entry)	**select 5 from DCE Main menu**
6	(No entry)	**type y to continue**
7	(No entry)	**select 99 from DCE Configuration menu**

3.7 ECS Assistant

This section covers the procedures necessary the System Administrator (SA) and/or Operator (OPR) to install new subsystem application software and monitor the system. This tool assists in the coordination and installation of software across multiple heterogeneous host machines.

ECS Assistant, is an easy-to-use GUI tool, has been developed to facilitate ECS SSI&T activities. Currently, the ECS Assistant is comprised of three major scripts: EcCoAssist, EcCoModemgr, and EcCoEsdtmgr. These scripts provide users with a Graphical User Interface to perform functions such as subsystem server startup and shutdown, ESDT management, and database review when using the ECS system. During the course of performing their tasks, SSI&T operators can use ECS Assistant to performs several functions through its GUI, which are listed in the **Activity Checklist** table.

Table 3.7-1. ECSAssistant - Activity Checklist

Order	Role	Task	Section	Complete?
1	SA	Install Subsystem Application Software	(I) 3.7.1	
2	SA/OPR	Start up and shut down servers for each subsystem	(P) 3.7.2	
3	SA/OPR	Graphically monitor the server up/down status	(P) 3. 7.3	
4	SA/OPR	Open and view the detailed log files for each server used	(P) 3. 7.4	
5	SA/OPR	Review various databases used in the ECS system	(I) 3. 7.6	
**		**Refer to Drop 4 Build Plan - Appendix D for**		
		Additional Information, if necessary		

In the following sections, we will address aspects of how to use the ECS Assistant in our SSI&T activities. This section explains how to use ECS Assistant to facilitate and manage the subsystems and their servers, including:

- server start up and shut down

- monitor servers for each subsystem, including using the ECS Monitor and ECS logfile viewer.

Table 3.7-2 outlines the assumptions that are required for all of the procedures defined in this section to operate properly.

Table 3.7-2. Assumptions - Checklist

Order	Role	Task	Section	Complete ?
1	SA	ECS Assistant has been properly installed.	ALL	
2	SA/OPR	Required environment variables have been set properly.	ALL	

3.7.1 Using ECS Assistant to Install Subsystem Software

Refer to the Drop 4 Build Plan - Appendix D

3.7.1.1 DCE CELLS

TBD

3.7.1.2 Making Config Parameter Files

Refer to the Drop 4 Build Plan - Appendix D

3.7.2 Using ECS Assistant to Start Up/Shut Down Servers

This procedure describes routings for using the ECS Assistant GUI to start up and shut down subsystem servers. The procedure described here will apply to all the servers from different subsystems.

To run the ECS Assistant, execute the procedure steps that follow:

Subsystem Server Start Up / Shut Down

1 Log into one of the host machines.

2 At the UNIX prompt on the host from which the ECS Assistant is to be run, type:
setenv DISPLAY *hostname*:0.0, press **Return**.

- The ***hostname*** is the name of the machine on which the ECS Assistant is to be displayed, *i.e.*, the machine that your are using.
- To verify the setting, type **echo $DISPLAY**, press **Return**.

3 At the UNIX prompt on the host from which the ECS Assistant is to be run, type:
setenv ECS_HOME /usr/ecs, press **Return**.

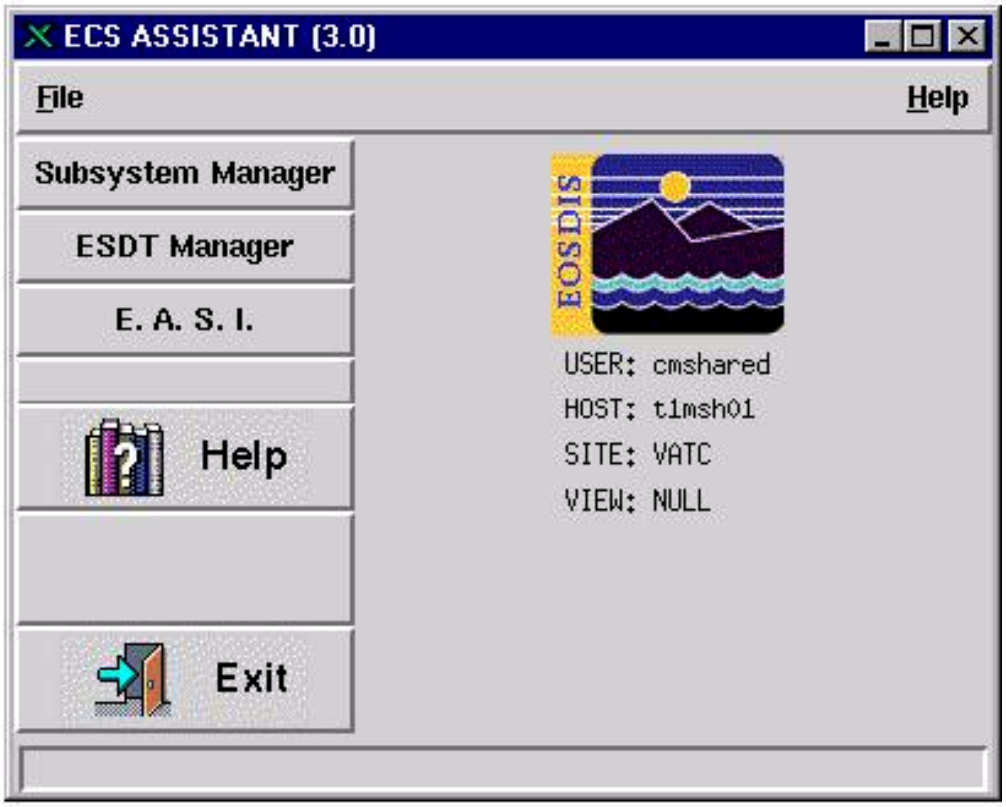
- To verify the setting, type **echo $ECS_HOME**, press **Return**.

4 If necessary, at the UNIX prompt on the host from which the ECS Assistant is to be run, type **cleartool setview *ViewName***, press **Return.**

- The ***ViewName*** is the ClearCase view to be used while the ECS Assistant is running in this session. For example, type **cleartool jdoe**, press **Return**.
- A ClearCase view is required only if the ECS Assistant needs to be able to see into a ClearCase VOB; a view is not necessary otherwise.

5 At the UNIX prompt, type **cd /tools/common/ea**, press **Return**. Then type:
EcCoAssist &, press **Return**.

- **/tools/common/ea** is the path where ECS Assistant is installed.
- This will invoke the ECS Assistant GUI with push buttons for selecting the proper activities, as indicated in Figure 3.7-1.

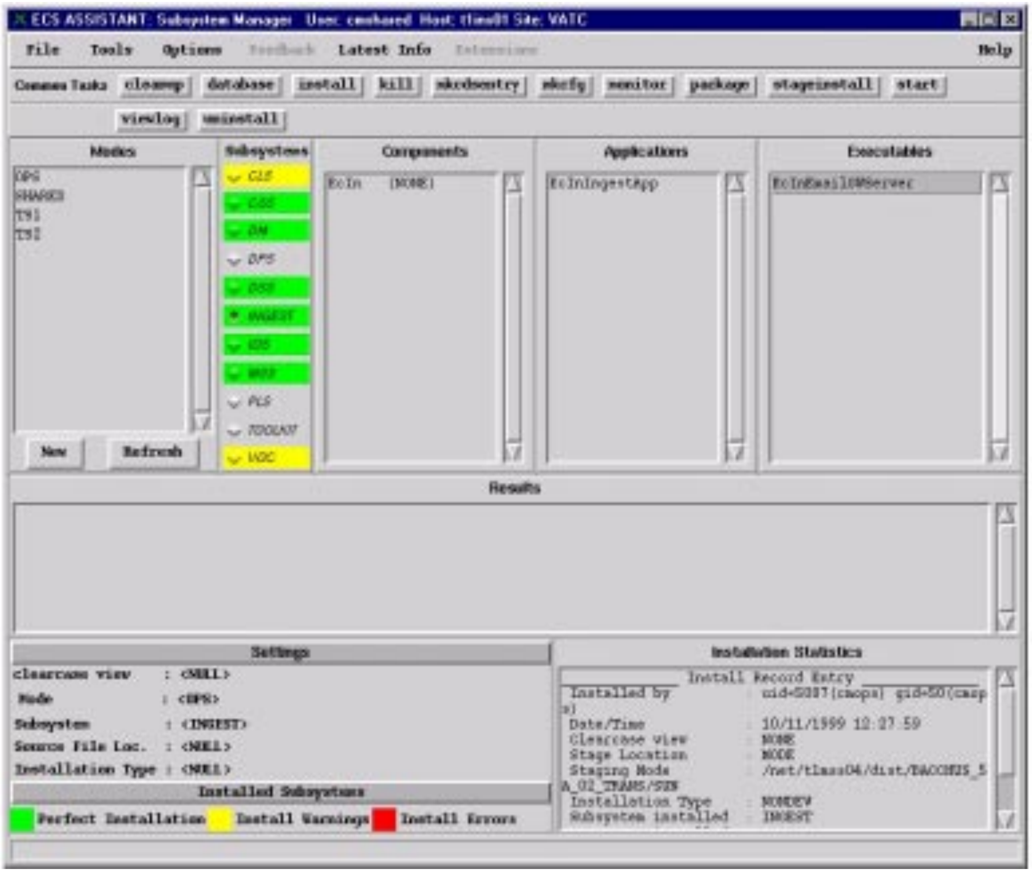


USER: cmshared
HOST: t1msh01
SITE: VATC
VIEW: NULL

Figure 3.7-1. ECS Assistant GUI

6 At the ECS Assistant GUI, click the **Subsystem Manager** pushbutton.

- This will invoke the Subsystem Manager GUI, as indicated in Figure 3.7-2.



```
OPS
SHARED
TS1
TS2
```

```
EcIn    (NONE)
```

```
EcInIngestApp
```

```
EcInEmailGWServer
```

```
clearcase view    : <NULL>
Mode              : <OPS>
Subsystem         : <INGEST>
Source File Loc.  : <NULL>
Installation Type : <NULL>
```

```
             Install Record Entry
 Installed by          : uid=5087(cmops) gid=50(cmop
s)
 Date/Time             : 10/11/1999 12:27:59
 Clearcase view        : NONE
 Stage Location        : NODE
 Staging Mode          : /net/t1ass04/dist/DAOOPS_5
A_02_TRANS/SUN
 Installation Type     : NONDEV
 Subsystem installed   : INGEST
```

Figure 3.7-2. Subsystem Manager GUI

7 Select a mode by clicking a mode in the mode listing.

- Once the mode is selected, the color of the subsystem name list is changed.

8 Select a subsystem with the **Subsystem** radio button.

- The component list for the selected subsystem will appear in the component window.

9 Select a component by clicking the component name under the component window.

- The selected component will be highlighted.
- The server list corresponding to that component will appear in the server window.

10 Select a server by clicking the server name from the server list under the servers window.

- The server selected is highlighted.

11 To start a server up or shut it down:

- Click the **start** button in the common tasks bar. This will start up the selected server.
- Click the **kill** button in the common tasks bar. This will shut down the selected server.

12 Repeat steps 7-11 to start up or shut down other servers.

13 To exit the Subsystem Manager GUI, select **File..Exit** in the menu bar of the Subsystem Manager GUI.

- This will terminate the Subsystem Manager GUI**.**

3.7.3 Using ECS to Perform System Monitoring

ECS Assistant provides two ways to monitor server status. The first one is by performing tail -f to log files which record the important activity history performed on the servers. The other way is by using a database table to display server up/down status' dynamically. These monitoring methods are described in the following sections.

3.7.3.1 Using ECS Assistant to Open / View Log Files for a Selected Server

Log files are used extensively in the ECS system to record a history of activity performed on the system. They provide useful information about server activities. ECS Assistant provides an easy way to access and view these log files. In the Subsystem Manager GUI, there is one button called **viewlog** in the Common Tasks bar. Click this button to invoke a log file GUI, as shown in Figure 2. You can review the log files for a particular server by choosing the server name from the Menu for the Subsystem to which it belongs. You can also view all of the log files for a component by choosing it in the Components menu. Menu entries are dimmed if no log files are present. The following example shows how to use this GUI to open log files for a particular server.

To run the Log Viewer, execute the procedure steps that follow:

1 Click the **viewlog** button in the Subsystem Manager GUI.

- This will invoke the log viewer GUI.

2 To open and view log files for a particular server, select a server from the Subsystem pull down menu, then click the server name.

- This will open all the log files corresponding to that server.
- The log file name is indicated in the title bar for each log file GUI.

3 The log file GUI provides the following options for users to view log file contents. Follow the guidance in the GUI to select the proper options:

- **Foreground color** for changing the foreground color.
- **Background** color for changing the background color.
- **Font size** for changing font sizes.
- **View entire file** for displaying the entire file.
- **Continuous update (tail -f)** for displaying the updated log file continuously.
- **Search for** for performing word searches in the log file.

- **Print** for printing the log file.

4 To view log files for other servers, repeat steps 1-3.

5 Exit the log file by pressing **EXIT**.

3.7.3.2 Using ECS Assistant to Monitor Server Status

ECS Assistant provides another convenient way to monitor the status of the servers by listing their up/down condition. The status flag for a server is up or down indicating whether or not that server is running.

To start up the ECS monitor GUI, execute the procedure steps that follow:

1 At the ECS **Subsystem Manager** GUI, select a mode by clicking a mode in the mode list.

- The mode should be the one to be used for SSI&T.
- Once the mode is selected, the color of the subsystem name list is changed.

2 Select a subsystem by clicking the radio button next to the subsystem name under the subsystem component window.

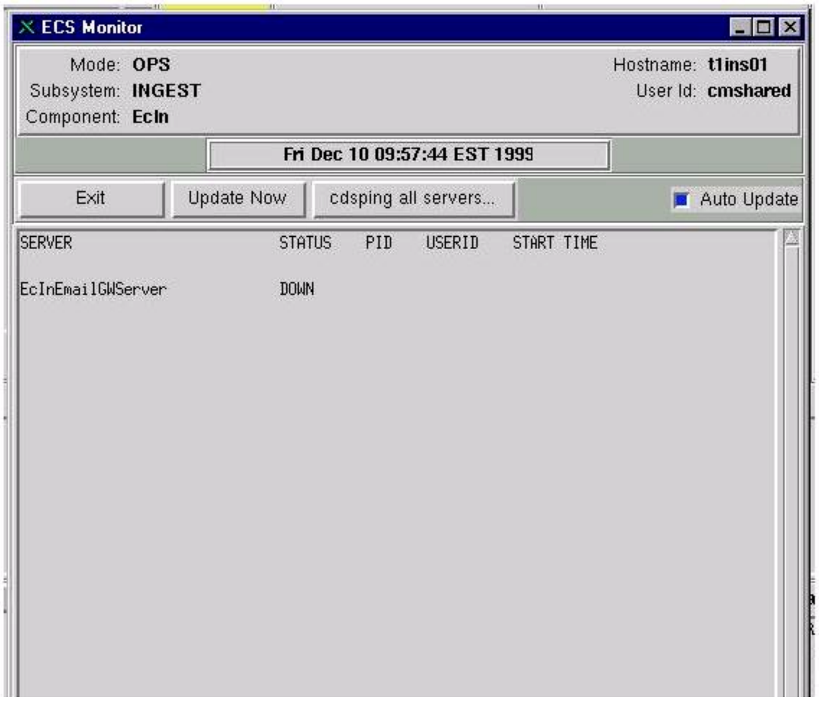
- The selected subsystem radio button will be highlighted.
- The components corresponding to that the subsystem will be displayed in the component window.

3 Select a component by clicking its name under the component window.

- All the servers for the selected component will be displayed in the server window.

4 If desired, click the **monitor** button from the common tasks window.

- This will invoke the ECS Monitor GUI window as shown in Figure 3.7-3.
- The status UP/DOWN indicates whether the server is running.



Mode: OPS
Subsystem: INGEST
Component: EcIn
Hostname: t1ins01
User Id: cmshared

Fri Dec 10 09:57:44 EST 1999

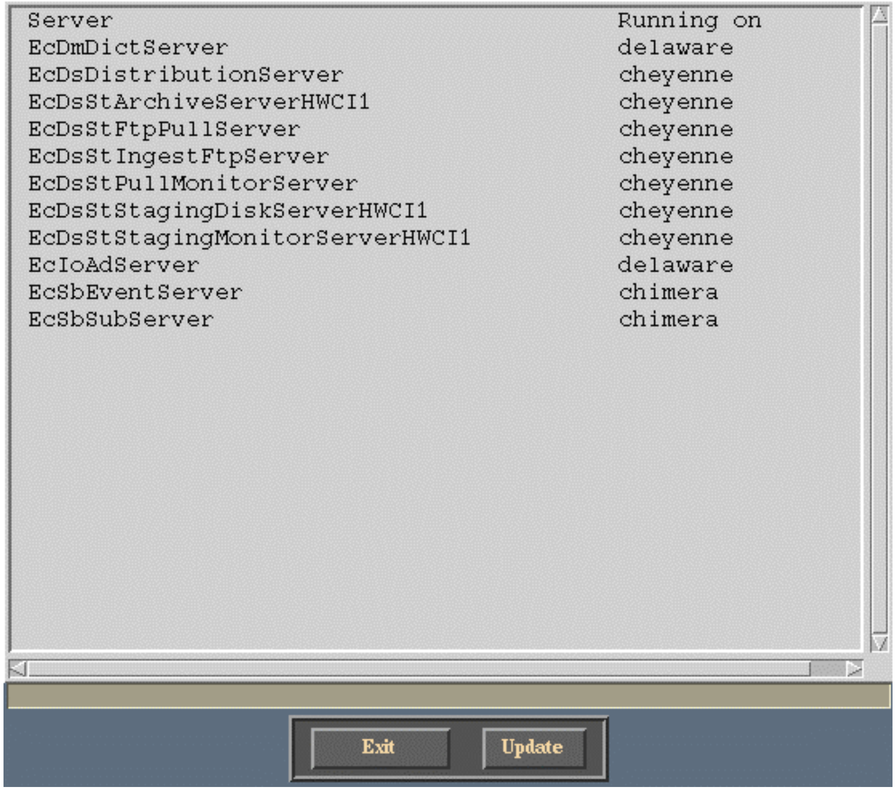
```
SERVER                        STATUS   PID   USERID   START TIME

EcInEmailGWServer             DOWN
```

Figure 3.7-3. Server Monitor GUI

5 To see which host each server is running on, click the **cdsping all servers** button.

- This will invoke the ECS Monitor (cdsping) GUI as indicated in Figure 3.7-4.
- The host name for each running server is listed



```
Server                                    Running on
EcDmDictServer                            delaware
EcDsDistributionServer                    cheyenne
EcDsStArchiveServerHWCI1                  cheyenne
EcDsStFtpPullServer                       cheyenne
EcDsStIngestFtpServer                     cheyenne
EcDsStPullMonitorServer                   cheyenne
EcDsStStagingDiskServerHWCI1              cheyenne
EcDsStStagingMonitorServerHWCI1           cheyenne
EcIoAdServer                              delaware
EcSbEventServer                           chimera
EcSbSubServer                             chimera
```

Figure 3.7-4. cdsping GUI

6 Both ECS monitor GUI and ECS Monitor (cdsping) GUI can be updated by clicking the **update** button in the GUI.

- This will cause the list to update to the current status.

7 To monitor other servers, repeat steps 2-4.

8 To exit, click the **EXIT** button.

- This will end the monitor GUI.

This page intentionally left blank.